
المعلومات وجالوت
المعارك الخفية لتجميع بياناتك
والسيطرة على عالمك
تأليف: بروس شناير
ترجمة: د. أحمد مغربي
منتدى العلاقات العربية والدولية

المعلُومات وجالُوت

حين تضع هاتفك في جيبك كل صباح، أنت تعقد صفقة غير مُعلَنة تقول: أريد أن أتبادل المكالمات مع الآخرين، وبالمقابل أسمح للشركة المصنِّعة أن تعرف أماكن وجودي بدقّة في كل الأوقات، ما يعني إبقائي تحت رقابتها الدائمة. إذا كان هاتفك ذكيّاً فهو عمليّاً حاسوب، وكل تطبيقاته تقدّم معلومات شخصيّة عنك، حين تستخدمه وحين لا تستخدمه. وإذا اتصلت بالإنترنت تتضاعف المعلومات عنك وعن أصدقائك وبرمجيّاتك وتعاملاتك وخياراتك فيما تشاهده وتسمعه وتقوله، وفي نهاية المطاف، تفكّر فيه.

لقد نشأت صناعة سمسرة معلومات كاملة تتركّز حول التكسّب من بياناتك، تُباع فيها معلوماتك الشخصيّة، دون معرفتك وبدون إذن منك، إلى شركات مختلفة، تبيعها بدورها إلى متاجر ومراكز تسوّق سيعرف موظّفوها اسمك وعنوانك ومستوى دخلك بمجرّد عبورك الباب، وتعرفك لوحات الإعلانات في الطرقات، ورفوف محلات البقالة، وتسجّل استجاباتك وتتعاون معاً لإغوائك باستهلاك المزيد. ويقود كل ذلك نموذج حوسبة جديد يجمع بياناتك الشخصيّة في "سحابة إلكترونيّة" تبقى هي أيضاً تحت سيطرة الشركات المُصنِّعة، ومن ورائها الحكومات.

لأول مرة في التاريخ الإنساني، كما تنبّأ جورج أورويل روائيّاً، وكشف إدوارد سنودن فعليّاً، تمتلك الحكومات القدرة على ممارسة رقابة شاملة ومنفلتة على شعوب بأكملها، داخل بلدانها وخارجها.

"كل مهتم بالحريّة والخصوصيّة والأمن في عصر الفضاء الإلكتروني يجب أن يقرأ هذا الكتاب".

جوزيف س. ناي الابن



هاتف: 44080451 974+ فاكس: 44080470 974+ صندوق بريد: 12231
الموقع الإلكتروني: fairforum.org البريد الإلكتروني: info@fairforum.org
العنوان: مبنى رقم 28، المؤسسة العامة للحي الثقافي (كتارا)، الدوحة، قطر

السعر:
50 ريالاً قطرياً - 14 دولاراً


ISBN: 978-9927-103-80-3

المعلومات وجالوت

المعارك الخفيّة لتجميع بياناتك والسيطرة على عالمك



بسم الله الرحمن الرحيم

المعلومات وجالوت

المعارك الخفية لتجميع بياناتك والسيطرة على عالمك

تأليف

بروس شناير

ترجمة

د. أحمد مغربي



Bruce Schneier, *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World*, New York & London: W. W. Norton Company, 2015.
© Bruce Schneier 2015

عنوان الكتاب: المعلومات وجالوت
المعارك الخفيّة لتجميع بياناتك والسيطرة على عالمك
تأليف: بروس شناير
ترجمة: د. أحمد مغربي
528 صفحة - 16.5 × 24 سم.
رقم الإيداع بدار الكتب القطرية: 2016/367
الرقم الدولي (ردمك): ISBN: 978-9927-103-80-3
جميع الحقوق محفوظة لمنتدى العلاقات العربية والدولية.
الطبعة الأولى 2017.

قيل في مديح كتاب **المعلومات وجالوت**:

«ثمة حاجة ماسة لكتاب **المعلومات وجالوت**. فبالإضافة إلى السيل الجارف من القصص المتواترة حول حروب الفضاء الافتراضي، واختراقات نُظُم المعلومات، والتجسس على الشركات، أثارت الأسرار التي كشف عنها [إدوارد] سنودن لدى كثيرين مشاعر الحيرة والمرارة حيال حماية خصوصيّتهم الشخصيّة. يحدوني الأمل بأن كتاب بروس شناير الجديد سوف يمكّن عامة الناس من المشاركة في النقاشات، داخل المحاكم وخارجها، حول كيفية التفكير بجدّية ونزاهة في الوضع الراهن للرقابة الإلكترونيّة، والأهم من ذلك كيفية بناء مجتمع رقمي يقوم على قبول المحكومين ورضاهم».

سندي كوهن، المستشارة القانونيّة لـ «مؤسّسة الحدود الإلكترونيّة»

«وضع بروس شناير كتاباً مهماً يحمل رؤىً ثاقبة إلى أبعد الحدود حول كيفية تأثير «البيانات الضخمة»، وابنة عمها «الرقابة العامة»، في حياتنا وما يمكننا فعله إزاءهما. على عادته، يأخذ شناير أفكاراً ومعلومات فائقة التنوّع والتعقيد، ويجعلها مفعمة بالحيويّة وسهلة الفهم ومقنعة لدرجة لا تقاوم».

جاك غولد سميث، الرئيس السابق لـ «مكتب الاستشارات القانونيّة» في وزارة العدل إبّان ولاية الرئيس جورج دبليو بوش

«الإنترنت حال من الرقابة التقنية، وككل تقنية، للرقابة استخدامات جيّدة وأخرى سيّئة. يستند بروس شناير إلى مهاراته التاريخية والتقنية الواسعة للتمييز بين هذين الحدّين، فيحلّل كلا التحدّي الذي تمثّله رقابة «الأخ الكبير»، ورقابة مجموعة «الإخوة الصغار». يتحتم على كل مهتم بالأمن، والحريّة، والخصوصيّة، والعدالة في عصر الفضاء الافتراضي الذي نعيشه أن يقرأ هذا الكتاب».

جوزيف س. ناي الابن، أستاذ الخدمة المميّزة في جامعة هارفرد، ومؤلّف كتاب **مستقبل السلطة**

«يعتبر بروس شناير الصوت الأكثر اتّزاناً وموثوقيّة واطّلاعاً بشأن قضايا الأمن والخصوصيّة في زمننا. ويقدّم الكتاب خبرة شناير ومهاراته التحليليّة الدقيقة لتقنية مهمة وسريعة التطور ولقضايا حقوق الإنسان المرتبطة بها. لقد قيل الكثير عن الطرق التي تعتمدها حكومتنا ومؤسّساتنا الماليّة وهيئاتنا الشبكيّة في جمع المعلومات. في المقابل، لم يُقَل سوى القليل عن كيفية استخدام ذلك المحيط اللامتناهي من المعلومات أو كيف يمكن استخدامه. في مواجهة مروحة واسعة من الخيارات الممكنة، والمغطاة بسحب السريّة، يشكّل كتاب بروس صوت المنطق المكين».

غزيني جاردن، المؤلّفة المشاركة للمُدوّنة الإلكترونيّة «بوينغ بوينغ»

«يشكّل كتاب المعلومات وجالوت دليلاً لا غنى عنه لفهم التهديد الأبرز للحريّة في المجتمعات الديمقراطيّة المرتكزة إلى حريّة السوق. سواء يعتريك القلق حول الرقابة الحكوميّة في عصر ما بعد سنودن، أم حول تلاعب شركتا «فيسبوك» و«غوغل» بك، اعتماداً على المجموعات الهائلة من المعلومات لديهما، فإنّ ما يكتبه شناير الاختصاصي والرائد والمستقل حقاً عن هذه التهديدات المعاصرة، يقدم نظرة شاملة وغنيّة عن التقنيّات والممارسات التي تقودنا صوب مجتمع الرقابة، والحلول المتنوّعة التي يجب أن نلجأ إليها لإنقاذنا من ذلك المصير».

يوشاي بِنكلر، أستاذ «بركمان للدراسات القانونيّة الاستثماريّة»
في كليّة القانون بجامعة هارفرد، ومؤلّف كتاب **ثروة الشبكات**

«تعطي البيانات والخوارزميّات والآلات المفكّرة شركاتنا ومؤسّساتنا السياسيّة قوى هائلة وواسعة التأثير. لقد أنجز بروس شناير عملاً مميّزاً في تحليل تلك القوى وتأثيرها في خصوصيّاتنا وحياتنا ومجتمعنا. يجب أن يوضع **المعلومات وجالوت** على رأس قائمة كل شخص للكتب الواجب قراءتها».

أوم ماليك، مؤسّس شركة «غيغاوم»

الإهداء

إلى كارين في مركز «دي إم إيه إس سي» (DMASC)

المحتويات

المعلومات(*) وجالوت(**)

مدخل

إذا أردت أن تقتنع بأنك تعيش في عالم من الخيال العلمي، فما عليك سوى النظر إلى هاتفك الخَلَوي. إذ بات ذلك الجهاز الجذاب والأنيق والخارق القوة مركزياً في حياتنا إلى حدّ أننا أصبحنا نسلّم بداهةً بوجوده. يبدو أمراً طبيعيّاً تماماً أن تُخرِج ذلك الجهاز من جيبك، بغض النظر عن مكان وجودك على كوكب الأرض، وتستخدمه للحديث مع شخص آخر، أيّاً كان موقعه على هذا الكوكب أيضاً.

لكن، في كل صباح تضع فيه الهاتف الخَلَوي في جيبك، أنت تعقد صفقة غير مُعلَنة تقول: «أريد أن أتبادل المكالمات بواسطة هاتفي الخَلَوي، وبالمقابل أسمح للشركة التي تعطيني خدمات الاتصال أن تعرف أمكنة وجودي بدقّة في كل الأوقات». لا تَرِد تلك المقايضة في أي عقد، لكنها متأصلة في طريقة عمل خدمات الخَلَوي. الأرجح أنك لم تفكّر بها من قبل، لكنك ربما صرت تفكر بها الآن بعد أن ذكرتها لك، وقد تعتقد أنها صفقة جيدة. الهاتف الخَلَوي حقيقةً ابتكار عظيم، لكنه لا يعمل دون أن تعرف شركات الخَلَوي مكان وجودك دوماً، ما يعني أنها تبقيك تحت رقابتها المستمرة.

(*) في علوم الكومبيوتر، هناك فارق كبير بين مصطلحي بيانات (Data) ومعلومات (Information)؛ لأن المعلومات هي ما يستخلص من البيانات، لكن ورد المصطلحان غالباً في الكتاب كأنهما متشابهان. (جميع الحواشي السفلية للمترجِم)

(**) لفظ "جالوت" (Goliath) وارد في القرآن الكريم ومستخدم في العربيّة الحديثة وبعض الكتب الدينيّة، مثله في ذلك مثل "غوليات".

هذا الشكل من الرقابة لصيق وحميمي جداً. إذ يتتبع الخَلَوي[1] أمكنة سكناك وعملك، والأمكنة التي تحب قضاء الأمسيات وعطل نهاية الأسبوع فيها. ويتتبّع وتيرة ذهابك إلى الكنيسة (ويحدّد أي كنيسة)، والمدّة التي تقضيها في «البار» [ويحدد أي «بار»]، وما إذا كنت تسرع أثناء قيادتك السيارة في الطريق إليهما. وبحكم معرفته عن كل الهواتف الأخرى في منطقتك، يتتبّع أيضاً الأشخاص الذين تقضي أيامك معهم، ومن تلتقيهم على وجبة الغداء، ومن تنام معهم. والأرجح أن تلك المعلومات المتراكمة[2] تستطيع أن ترسم صورة عن كيفية قضاء وقتك بأفضل مما تستطيع أنت؛ لأنها ليست مضطرة للاستعانة بالذاكرة البشريّة. في عام 2012، كان باستطاعة الباحثين[3] استخدام هذه المعلومات لتوقع أين سيقضي الناس أوقاتهم في *الـ24 ساعة التالية*، ضمن مسافة 20 متراً.

قبل الهواتف الخَلَوية، إذا رغب شخص ما في معرفة تلك المعلومات كلها، لربما وجب عليه أن يستأجر محقّقاً خاصاً كي يلاحقك باستمرار مسجّلاً الملاحظات عنك. باتت تلك مهنة بالية الآن؛ إذ يقوم الخَلَوي المستقر في جيبك بكل تلك الأمور أوتوماتيكياً. قد لا يستخرج أحد تلك المعلومات، لكنها موجودة بتصرف من يلتقطها.

المعلومات عن أمكنة وجودك قيّمة، والكل يسعى للوصول إليها. الشرطة تريدها؛ إذ يساعد تحليل المعلومات[4] المكانية في التحقيقات الجنائيّة بطرق متنوّعة. وتستطيع الشرطة[5] أن «ترن» على هاتف معيّن لتحديد مكانه، وتستعمل معلومات تاريخية لتحديد الأمكنة التي كان فيها قبل ذلك، وجمع كل «البيانات المكانيّة» عن الهواتف في منطقة معينة كي تعرف الأشخاص الذين كانوا فيها وأوقات وجودهم. أصبح رجال الشرطة يستخدمون معلومات الخَلَوي[6] لتحقيق تلك الأهداف بصورة مطّردة.

وتستعمل الحكومات أيضاً المعلومات عينها من أجل الترهيب والسيطرة الاجتماعيّة. في 2014، بعثت الحكومة الأوكرانيّة[7] بالرسالة النصيّة التاليّة التي لا يخفى طابعها الأورويلي[*]: «عزيزي المشترك، جرى تسجيلك كمشارك في شغب جماعي». لا يذهب بك الظنّ بأن ذلك السلوك يقتصر على البلدان التي تحكمها نُظُم شمولّية وحدها؛ ففي العام 2010، سعت شرطة ولاية «ميشغن»[8] إلى الحصول على أرقام هواتف كل من تجمّعوا بالقرب من مكان إضراب عمالي متوقّع، ولم تكترث بالحصول على مذكرة قضائيّة في ذلك الشأن.

هناك صناعة كاملة مكرّسة للحصول على معلومات تتعقب أمكنة وجودك على مدار الساعة، وفي الوقت الحقيقي الجاري. وتستعمل الشركات هاتفك الخَلَوي[9] لتتبع المخازن التي تتسوّق منها كي تتعرف إلى طريقتك في الشراء، وتتبعك في الطرقات كي تعرف إمكان وجودك قرب مخزن محدد، لترسل لك إعلاناً على الهاتف استناداً إلى البيانات عن أمكنة وجودك.

صارت «البيانات المكانيّة» قيّمة جداً[10]، إلى حدّ أن شركات الخَلَوي باتت تبيعها إلى سماسرة المعلومات، الذين يبيعونها بدورهم إلى كل راغب في الدفع مقابل الحصول عليها. وتتخصّص شركات كـ «سينس نِتوركس»[11] (Sense Networks) في صنع «بروفايل» شخصي عن كل منا، استناداً إلى ذلك النوع من المعلومات.

ليست شركات الخَلَوي المصدر الوحيد للمعلومات عن الهواتف. إذ تبيع شركة «فيرنت»[12] (Verint) نُظُماً لتعقّب الخَلَوي إلى شركات وحكومات في العالم كله. وعلى موقعها الشبكي[13]، تصف الشركة نفسها بأنّها «رائد عالمي في حلول الذكاء العملاني لضمان الحدّ الأقصى من مشاركة العملاء، والأمن الاستخباراتي، ومنع الاحتيال والمخاطر وفرض التجاوب والإذعان»، مع زبائن لها في «ما يزيد على

(*) إشارة إلى رواية الكاتب جورج أورويل الشهيرة 1984 التي رسم فيها صورة مجتمع يجري التحكّم به بواسطة رقابة مرئيّة- مسموعة مستمرّة.

عشرة آلاف منظّمة في أكثر من 180 بلداً». وتبيع شركة «كوبهام» (Cobham) البريطانيّة نظاماً يتيح إرسال مكالمة «عمياء» إلى أي هاتف خَلَوي[14]؛ بمعنى أنها لا تجعل الهاتف يرن، وليس بالمستطاع استشعارها. وترغم المكالمة العمياء الهاتف الذي يستقبلها على التجاوب معها بموجة ذات تردّد معين، ما يجعل المرسل قادراً على تحديد مكان الخَلَوي المستقبل، ضمن مسافة لا تتعدى متراً واحداً. وتفاخر الشركة[15] بأن لها زبائن حكوميّين في الجزائر وبروناي وغانا وباكستان والسعودية وسنغافورة والولايات المتّحدة. وتبيع شركة أخرى اسمها «دِفبتِك» (Defebtek)[16]، وهي مؤسّسة غامضة مسجّلة في جزيرة بنها، نظاماً معلوماتيّاً تقول الشركة إنه «يستطيع تحديد أرقام الهواتف في العالم بأسره وملاحقتها... من دون أن تشعر به شبكات الخَلَوي، ولا مقدّمو خدماتها، ولا المتلقي». وليست تلك الكلمات مجرد تفاخر فارغ، فقد برهن الباحث في الاتّصالات توبياس إنغل[17] على الأمر نفسه في أحد مؤتمرات قراصنة الكومبيوتر («هاكرز»/ Hackers(*)) في العام 2008. ويفعل مجرمون كثر الأمر عينه حالياً.

تعتمد كل نُظُم التتبّع المكاني هذه على النظام الخَلَوي. لكن هناك نظام آخر مختلف كليّاً، وأكثر دقّة في تحديد الأماكن، موجود في هاتفك الذكي: نظام تحديد المواقع جغرافياً في العالم، واختصاراً «جي بي إس» (GPS). إنّه النظام الذي يوفر المعلومات المكانيّة للتطبيقات الرقميّة المختلفة الموجودة على هاتفك. وتستخدم بعض تلك التطبيقات معلومات الـ«جي بي إس» في تقديم خدماتها، مثل «خرائط غوغل» (Google Maps)، و«أوبر» (Uber) و«يلب» (Yelp). فيما تسعى تطبيقات أخرى، مثل «آنغري بيردز» (Angry Birds)، إلى مجرد القدرة على تجميعها ثم بيعها[18].

تستطيع أنت أيضاً فعل الأمر نفسه، فـ«هيلو سباي» (HelloSpy)[19] تطبيق يمكنك تسريبه خفية إلى هواتف الآخرين الذكية كي تتتبّع حامليها، وهو خيار مثالي

(*) هو المتمرّس بالكومبيوتر بما يمكنه من اختراق حواسيب الآخرين.

لأم قلقة تود معرفة الأماكن التي يرتادها ابنها المراهق، أو لرجل سيئ يرغب في التجسّس على زوجته أو صديقته[20]. كما استخدم بعض المديرين تطبيقات رقميّة مشابهة للتجسّس على موظّفيهم[21].

تستعمل وكالة الأمن القومي في الولايات المتحدة (US National Security Agency)، ونظيرتها البريطانية، «مركز قيادة الاتّصالات الحكوميّة» (Government Communications Headquarters)، المعلومات المكانية لتتبّع عامة الناس. وتجمع وكالة الأمن القومي البيانات المكانيّة للهواتف الخَلَوية[22] من مصادر متنوّعة: أبراج الخَلَوي التي تتصل بها الهواتف، وشبكات الـ «واي- فاي» التي تدخل إليها، ومواقع الأمكنة التي تحدّدها تقنية الـ «جي بي إس» بواسطة تطبيقات الإنترنت. وتحتوي اثنتان من قواعد البيانات في وكالة الأمن القومي، تحملان اسمين حركيّين هما «هابي فووت» (HAPPY FOOT) و«فاس- سي آي إيه» (FAS- CIA)، معلومات شاملة عن مواقع الهواتف عالميّاً. وتستخدم الوكالة قواعد بياناتها لتتبع تحرّكات الناس، ورصد من يلتقون بأشخاص تهتم بأمرهم، وكذلك توجيه أهداف الطائرات من دون طيّار («درون»/ Drone).

يقال أيضاً إن وكالة الأمن القومي تستطيع تتبع الهواتف الخلوية حتى حين تكون مغلقة[23].

لم يطل حديثي حتى الآن سوى «البيانات المكانيّة» التي تُجمع من مصدر واحد- جهازك الخلوي - لكن القضية أوسع من ذلك بكثير. الحواسيب التي تتعامل معها تنتج على الدوام معلومات شخصيّة حميمة عنك. وتتضمن ما تقرأه، وتشاهده، وتستمع إليه. وتشمل من تتحدث إليه، وما تقوله له. وتغطي في النهاية ما تفكر به، على الأقل بمقدار ما تقودك أفكارك إلى الإنترنت ومحرّكات البحث فيها. نحن فعلاً نعيش العصر الذهبي للمراقبة[24].

قالها سكوت ماكنيلي، الرئيس التنفيذي لشركة «صن مايكروسيستمز» (Sun Microsystems) بوضوح تام قبل زمن بعيد في عام 1999: «لديك صفر خصوصيّة[25] في كل الأحوال. انسَ الأمر». هو مخطئ بالطبع حول ردة فعلنا على الرقابة وما يجب عمله إزاءها، لكنه محقّ تماماً في أن الحفاظ على الخصوصيّة وتجنّب الرقابة يغدوان أكثر صعوبة باطراد.

الرقابة مصطلح مثقل بالدلالات السياسيّة والعاطفيّة، لكنني أستعمله عامداً. إذ يُعرِّف الجيش الأميركي الرقابة[26] بأنها «ملاحظة ممنهجة». وكما سأوضح، ينطبق ذلك التعريف تماماً على الرقابة الإلكترونيّة المعاصرة. نحن كُتُب مفتوحة بالنسبة للحكومات والشركات، وقدرتها على التمعن في حياتنا الشخصيّة الجمعية أضخم مما كانت عليه في أية فترة سابقة.

أكرر القول ثانية: إنّ الصفقة التي تجريها مع شركات متنوّعة هي الرقابة مقابل الحصول على خدماتها الحرّة. في كتابهما المشترك **العصر الرقمي الجديد** (New Digital Age)، رسم إريك شميدت، رئيس شركة «غوغل»(*)، ويارد كوهن، رئيس «قسم الأفكار» فيها، صورة تلك الصفقة. وهنا، أعيد صوغ رسالتها: «إذا سمحت لنا بالحصول على جميع معلوماتك[27]، فسوف نريك إعلانات ترغب في رؤيتها، وسنهبك مجاناً القدرة على البحث المفتوح في الإنترنت والبريد الإلكتروني وكل أنواع الخدمات الأخرى». إنه تبادل مصالح أساساً. نحن البشر حيوانات اجتماعيّة، ولا شيء يعادل مكافأتنا ويؤثر فينا كالتواصل مع الآخرين. باتت الوسائل الرقميّة الطريقة الأسرع والأسهل في الاتّصال. لكن لماذا نسمح للحكومات بالوصول إلى معلوماتنا؟ لأننا نخاف الإرهابيّين، ونخاف أن يختطف الغرباء أطفالنا، ونخاف مهرّبي المخدرات، ونخاف الأشرار من كل نوع ومن آخر صنف رائج حالياً.

(*) تعرف تلك الشركة الآن باسم "ألفا بيت" (Alphabet)، وتسميتها «غوغل» رائجة.

إنّـه التبريـر الذي تقدّمه «وكالـة الأمن القومـي» لبرامجها في الرقابة العامـة[28]: إذا سمحت لنا بالحصول على معلوماتك كافة، فلسوف نتكفل بإزاحة الخوف عنك.

المشـكلة أنّ تلك الصفقات ليسـت جيّـدة ولا عادلة، على الأقـل بالطريقة التي يجـري ترتيبهـا اليوم. لقد درجنا على قبولها بسـهولة زائدة، ومـن دون أن نفهم حقاً بنودها وشروطها.

إليك ما هو حقيقي. إن التكنولوجيا الرقميّة اليوم تعطي الحكومات والشركات قدرات جبارة على الرقابة العامة. والرقابة العامة خطرة. فهي تمكّن التمييز اسـتناداً إلى أية معايير تقريباً: العرق والدين والطبقة والمعتقدات السياسيّة. ويجري استخدام تلـك الرقابة في السـيطرة على مـا نراه، وما نسـتطيع فعله، وبالنتيجة عـلى ما نقوله. كـما يجري اسـتخدام تلك الرقابة مـن دون منح المواطنين أي حمايـة أو قدرة حقيقية عـلى الاختيـار أو الرفض، ومـن دون وجود ضوابـط وتوازنات كافيـة. إنّها تجعلنا أقـل أماناً، وأقـل حريّة. والقوانين التـي وضعناها لحمايتنا من هـذه المخاطر في نُظُم التقنيّـات السـابقة، صارت غير كافيـة إلى حد كارثي؛ بل إنها غـير فعّالة ولا تعمل. نحن بحاجة لإصلاح ذلك، وإصلاحه سريعاً جداً.

في الكتاب الحالي، أقيم تلك الحجة في ثلاثة أجزاء.

يصـف الجزء الأول مجتمع الرقابة الذي نعيش فيه. يدقّق الفصل الأول في أنواع المعلومـات الشـخصيّة التـي نولّدها أثنـاء حياتنـا. ولا يقتصر الأمر عـلى «البيانات المكانيّة» التي أتيت على ذكرها سـابقاً في الهاتف الخَلَوي. هناك أيضاً المعلومات عن مكالماتنا الهاتفيّة العادية، وبريدنا الإلكتروني، ورسـائلنا النصيّة القصيرة، إضافة إلى صفحـات الإنترنـت التي نقرؤها، والمعلومـات عن معاملاتنا الماليّة، وأشـياء كثيرة أخـرى. لا يـدرك معظمنا المدى الذي باتت فيها الحواسـيب منبثّـة في كل ما نفعله، أو الكلفة المتدنية لتخزين المعلومات على الكومبيوتر إلى حد جعل من الممكن حفظ

كل البيانـات التـي تتدفّق منـا إلى ما لا نهاية. كذلك يقلّل معظمنا من السـهولة التي صارت عليها عملية التعرّف إلينا باستخدام معلومات نعتقد أنها طيّ الكتمان.

يُظهِر الفصل الثاني كيف تستعمل كل تلك المعلومات لأغراض الرقابة. وكيف تحـدث في كل مـكان، بصـورة أوتوماتيكيّـة، مـن دون تدخّـل بشري، وبعيـداً عن الأعين. إنها الرقابة العامة كليّة القدرة.

من السـهل التركيز على طريقة جمع المعلومات مـن قِبَل الحكومات والشركات، لكن ذلك يعطي صورة مشوّهة. تكمن القصة الحقيقية في كيفيّة معالجة تلك السيول مـن البيانات، وربطها وتحليلها. وليس معلومات عن شـخص بعينه، بل معلومات عـن الجميـع. الرقابة الشـاملة تختلف جذرياً عـن تجميع كثير من معلومـات الرقابة الفرديّة، وتحصل على مدى لا نظير له من قبل. سأتحدّث عن ذلك في الفصل الثالث.

تُجمَـع بيانـات الرقابـة بشـكل رئيـس مـن شركات نتعامـل معهـا كزبائـن أو مسـتَخْدمين. يتنـاول الفصـل الرابـع نـماذج الرقابـة التجاريّة، خصوصـاً الإعلان المُشَخْصَن (Personalized Advertisement). لقد نشأت صناعة سمسرة معلومات كاملـة تتركز حول التكسـب من بياناتنا، وتُباع فيها معلوماتنا الشـخصيّة وتشـترى دون معرفتنـا وبـلا إذن منّا. ويقـود ذلك حالياً نمـوذج جديد من الحوسـبة، قوامه تجميـع بياناتنا في «سـحابة»، يجري الدخول إليها بواسـطة أجهزة كـ«آي فون»، هي أيضاً تبقى تحت السـيطرة اللصيقة للمُصَنِّع. وبالنتيجة، صارت الشركات تسـتطيع الوصول إلى معلوماتنا الأكثر حميميّة والسيطرة عليها بشكل غير مسبوق.

يلتفت الفصـل الخامس إلى قضية الرقابة الحكوميّة. كل حكومات العالم تفرض رقابة على مواطنيها، وتقتحم حواسيبهم محليّاً ودولياً. ترغب الحكومات بالتجسس عـلى الجميع للوصـول إلى المجرمـين والإرهابيّين وكذلك -تبعـاً لنوعية الحكومة- النشـطاء السياسـيّين والمنشـقين ونشـطاء البيئـة والمدافعـين عن حقوق المسـتهلك

والمفكّرين الأحرار. أركّز بشكل رئيس على «وكالة الأمن القومي» لأنها الوكالة الحكوميّة السريّة التي بتنا نعرفها أكثر من غيرها، بسبب تسرّب وثائق سنودن.

تتساوى الحكومات والشركات في امتلاك شهية لا تشبع لمعلوماتنا، وسأناقش كيف يعمل الطرفان معاً في الفصل السادس. أسمّي ذلك «شراكة القطاعين العام-الخاص في الرقابة»، وذلك تحالف عميق الغور. إنه السبب الرئيس في جعل الرقابة واسعة الانتشار، وإعاقتها محاولات إصلاح النظام.

كل هذه الأمور مهمّة، حتى لو كنت تثق بالشركات التي تتعامل معها والحكومة التي تعيش في ظلها. مع أخذ ذلك بالاعتبار، يتناول الجزء الثاني الرقابة العامة الشاملة، مبيّناً الأضرار التي تنجم عنها.

في الفصل السابع، أناقش الأضرار التي تنجم عن رقابة الحكومة. إذ بيّن التاريخ تكراراً الأضرار المتأتية من السماح للحكومة بممارسة رقابة عامة منفلتة على مواطنيها. تشمل قائمة الأضرار المحتملة السيطرة على المواطنين والتمييز بينهم، والآثار المرعبة على حريّة التعبير والفكر، والإساءة الحتمية لاستخدام السلطة، وضياع الحريّة والديمقراطيّة. تملك الإنترنت قدرة كامنة في أن تكون محرّكاً ضخماً للحرية والتحرّر عالمياً، لكننا نبدد تلك الإمكانيّة بالسماح للحكومات بممارسة رقابة عالميّة شاملة.

يلتفت الفصل الثامن إلى الأضرار الناجمة عن انفلات رقابة الشركات. إذ باتت الشركات حاضراً تُحكِم سيطرتها على «أمكنة» تجمّعنا على الإنترنت، وتُنقّب في المعلومات التي نتركها هناك، كي توظّفها لمصلحتها. وبسماحنا للشركات بأن تعرف كل شيء عنّا، فإننا نتيح لها أن تصنّفنا وتتلاعب بنا. يجري ذلك التلاعب في الخفاء ومن دون قوانين، وتزداد فعاليته مع تطوّر التقنية.

تؤدّي الرقابة الشاملة إلى أنواع أخرى من الأضرار. يبحث الفصل التاسع الاقتصادية منها، أساساً على الأعمال الأميركيّة، وهي تحدث عندما يحاول مواطنو

دول مختلفة حماية أنفسهم من رقابة وكالة الأمن القومي وحلفائها. تمثّل الإنترنت منصّة عالميّة، وسوف تتسبّب المحاولات التي تبذلها بلدان كألمانيا والبرازيل لبناء جدران وطنيّة حول معلوماتها، بأضرار مكلفة للشركات التي تتيح للحكومات أن تمارس الرقابة، خصوصاً الشركات الأميركيّة.

في الفصل العاشر، أناقش الأضرار التي يتسبّب بها ضياع الخصوصيّة. إنّ أنصار الرقابة- من وكالة الاستخبارات الألمانيّة الشرقيّة التي اشتُهِرَت باسم «ستازي» (Stasi)، إلى ديكتاتور تشيلي السابق الجنرال أوغستو بينوشيه، إلى مدير «غوغل» إريك شميدت- اتّكأوا دوماً على القول المأثور «إذا لم يكن لديك ما تخبّئه، فليس لديك ما تخشاه». يجسّد ذلك القول مفهوماً ضيّقاً بشكل خطير لمفهوم الخصوصيّة. إذ إن الخصوصيّة هي حاجة إنسانيّة أساس، وهي مركزيّة لقدرتنا على التحكّم بالطريقة التي نتفاعل بها مع العالم. والحرمان من الخصوصيّة يحط من إنسانيّة البشر بشكل أساسي، ويتساوى في ذلك أن يلاحقنا مخبر شرطة سري، أو أن ترصد جداول حسابات («خوارزميّات» / Algorithms[*]) في الكومبيوتر كل تحرّك نأتي به.

في الفصل الحادي عشر، ألتفتُ إلى الأضرار التي تلحقها الرقابة بالأمن. غالباً ما تصوّر الرقابة الحكوميّة العامة باعتبارها مكسباً أمنيّاً، وشيئاً يحمينا من الإرهاب. على الرغم من ذلك، لم يقم دليل فعليّ على نجاحات حقيقيّة للرقابة الشاملة حيال الإرهاب، في مقابل وجود أدلة مهمة على حدوث أضرار بسببها. الحال أن التمكّن من ممارسة رقابة شاملة، يفرض الإبقاء على الإنترنت غير آمنة، ما يجعلنا جميعاً أقل أمناً تجاه الحكومات الأخرى المُنافِسة، وتجاه المجرمين وقراصنة الحواسيب («هاكرز»).

(*) التسمية مشتقّة من اسم عالم الرياضيّات محمد الخوارزمي، وهو مؤسّس علم الجبر أيضاً. وتعمل الجداول الخوارزميّة على تقديم حلول لمسائل رياضيّة معقّدة بتبسيطها إلى خطوات متتالية يضبطها نظام معيّن للأرقام.

في الختـام، يرسـم الجـزء الثالث ما يجب علينـا فعله كي نحمي أنفسـنا من رقابة الحكومات والشركات. إنّ المعالجات معقّدة بقدر القضايا المتّصلة بالرقابة الشاملة، وتتطلّـب تنبّهـاً جيّـداً للتفاصيل. مع ذلـك، وقبل الدخـول إلى التوصيـات التقنيّة المحدّدة وتلك المتعلقة بالسياسـات تجاه الرقابة، يقدّم الفصل 12 ثمانية مبادئ عامة توجه تفكيرنا في تلك المسألة.

يضع الفصلان التاليان توصيات محدّدة في مجال السياسة الواجب اتباعها، للحكومة (الفصـل 13) وللشركات (الفصل 14). تتضمن بعض التوصيات تفاصيل أكثر من بعضهـا الآخر؛ ويميل بعضها لأن يكون طموحاً أكثر من كونه عمليّاً وقابلاً للتنفيذ. لكن كل التوصيّات مهمّة، وقد تضر أية حذوفات بالحلول الأخرى.

ينتقـل الفصل 15 إلى ما يمكن لكل منـا فعله فرديّاً. أُقدم بعض النصائح التقنية المفيدة عملياً، بالإضافة إلى مقترحات لما يمكن فعله سياسـيّاً. نعيش في عالم تستطيع التقنية فيه أن تتغلب على السياسـة، كما يمكن للسياسـة أن تتغلب على التقنيّة، لكننا نحتاج أن يعمل كلاهما معاً.

اختتـم الفصـل 16 بالتفكـير في ما يمكـن أن نفعله بصـورة جماعيّـة كمجتمع. تتطلّـب معظـم توصيـات الفصلين 13 و14 إجـراء نقلـة في طريقة فهمنـا للرقابة وأهمية الخصوصيّة؛ لأننا لن نتوصل إلى إجراء إصلاحات قانونيّة مهمّة، من دون أن يطالـب المجتمع بها. هناك فائدة كبرى مـن تجميع معلوماتنا لغايات البحث الطبي، وتطوير التعليم، ووظائف أخرى مفيدة للمجتمع. يجب أن نعرف كيف نستفيد من ذلك جماعيّاً، مع تقليص الأضرار. هذه هي القضية الأساس التي يرتكز عليها إليها كل شيء في هذا الكتاب.

يشـمل الكتاب أشـياء كثيرة، مـا يعني أن تغطيتـه سريعة بالـضرورة. وتتضمّن الملاحظـات الختاميّـة مراجـع موسّـعة للمهتمـين بالتعمـق في الأمـور. تتوافر تلك الملاحظات أيضاً على الموقع الشـبكي للكتـاب (www.schneier.com /dg.html).

تجـد أيضاً في الموقع تحديثات للكتاب، اعتماداً على حوادث وقعت عقب انتهائي من كتابة مخطوطته.

أكتـب بتحيـز شـديد للولايـات المتّحدة. إذ تـأتي معظـم الأمثلة مـن الولايات المتّحـدة، وتنطبق معظم التوصيّـات نموذجياً على الولايـات المتّحدة. ويرجع ذلك إلى أمر أسـاس هو أن الولايات المتّحدة هي البلد الذي أعرفه. لكنني أعتقد أيضاً أن الولايات المتّحدة تصلح مثالاً متفرّداً عن الطريقة التي سـلكت فيها الأمور مسـاراً خاطئاً، وهي في وضع متفرّد لتغييرها نحو الأحسن.

خلفيتي في الأمن والتكنولوجيا. كتبتُ لسـنوات طويلة عن كيفيّة تأثير التقنيّات الأمنيّة في حياة الناس، والعكس بالعكس. راقبت صعود الرقابة في عصر المعلوماتيّة، ملاحظـاً المخاطـر الكثيرة وانعدام الأمن في هذا العالم الجديـد. تعوّدت على التفكير في المسـائل الأمنيّة، ونظرت إلى القضايا الاجتماعيّة الأوسع نطاقاً بعدسة المشكلات الأمنيّة. وقد منحني ذلك المنظور فهماً متفرّداً للمشكلات والحلول معاً.

لسـت مناهضـاً للتكنولوجيـا، وليـس الكتـاب مناهضاً لهـا أيضاً. لقـد جلبت الإنترنـت، والعـصر المعلومـاتي عمومـاً، منافـع ضخمـة للمجتمـع. وأعتقـد أنهما سيسـتمران في ذلك. لسـت حتى مناهضـاً للرقابة. لقد سـاهمت المنافـع المتأتيّة من معرفـة الكومبيوترات لما نفعلـه في إحداث تحول في الحياة بأسرهـا. أحدثت الرقابة ثـورة في المنتجات والخدمـات التقليديّة، وأطلقت أنواعاً جديـدة كليّاً من التجارة، وصارت كذلك أداة لا تقدر بثمن في دعم القانون وإنفاذه. إنها تساعد شعوب العالم بطُرُق عديدة، وستستمر بفعل ذلك لفترة طويلة مستقبلاً.

لكن مخاطر الرقابة حقيقيّة، ولا نتحدث عنها بصورة كافية. ردة فعلنا على هذه الرقابة الزاحفة سلبيّة عموماً، فنحن لا نفكّر بالصفقات التي نعقدها؛ لأن أحداً لم يضعها أمام أعيننـا بوضوح بتلك الصيغة. تحدث التغـيّرات التقنية ونتقبل معظمها، ويصعب إلقاء

اللـوم علينـا، فالتغيّرات تحدث بسرعة فائقـة إلى حدّ أننا لم نقيّم حقـاً تأثيراتها أو نوازن عواقبها. هكذا انتهينا إلى العيش في مجتمع الرقابة الذي تسلل خفية إلينا.

يجـب ألا تكـون الأمور على ذلك النحو، لكن علينا تولي الأمور بأنفسـنا. يمكن أن نبـدأ بإعادة التفاوض حـول الصفقات التي نعقدها بمعلوماتنـا. علينا أن نكون فاعلـين في طُرُق تعاملنا مـع التقنيّات الجديدة. وعلينا التفكير في ما نرغب أن تكون عليه بنيتنا التحتيّة تقنيّاً[29]، وما القيم التي نرغب أن تجسّدها. علينا أن نوازن أهمية معلوماتنـا للمجتمـع بطابعها الشـخصي. وعلينـا أن نتفحص مخاوفنـا، ونقرر بكم مـن خصوصيتنا نحن مسـتعدون للتضحية مقابل راحتنا. علينـا أن نتفهم الأضرار العديدة للرقابة المفرطة.

وعلينا أن نقاوم.

منيابوليس، ولاية مينوسوتا،
وكيمبردج، ولاية ماساتشوستس
تشرين الأول (أكتوبر) 2014

الجزء الأول

العالم الذي نصنعه

1

المعلومات منتجاً جانبياً للحوسبة

تنتج الحواسيب المعلومات بصورة مستمرة، فهي مُدخلاتها ومُخرجاتها. لكن المعلومات أيضاً منتج جانبي لكل ما تقوم به الحواسيب، التي توثّق على الدوام كل ما تفعله في سياق عمليّاتها الاعتيادية، بل تحسّ وتسجّل أشياء تفوق إدراكنا لها.

يحتفظ برنامج مُعالَجة الكلمات، مثلاً، بسجلّ عن كل ما تطبعه، بما في ذلك المسوّدات والتغيّرات في النصوص كلها. عندما تضغط على زر «حفظ»، يسجّل مُعالِج الكلمات النسخة الجديدة، لكنه لا يمسح النُسَخ القديمة إلا إذا احتاج مساحة التخرين التي تحتلها كي ينجز عملاً آخر. كما يحفظ مُعالِج الكلمات وثائقك أوتوماتيكيّاً على نحو متكرّر. برنامج «مايكروسوفت وورد» يحفظ وثائقي الخاصة كل 20 دقيقة، ويحتفظ بسجل عمن صنع تلك الوثائق، وغالباً كل من اشتغل عليها أيضاً.

اتّصل بالإنترنت، فيتضاعف إنتاجك للبيانات التي تشمل سجلات المواقع التي زرتها، والإعلانات التي نقرت عليها، والكلمات التي طبعتها. كذلك تُنتَج المعلومات من حاسوبك، والمواقع التي زرتها، والحواسيب التي دخلت عليها عبر الشبكة. إذ يرسل برنامج تصفّح الإنترنت الذي تستعمله بيانات إلى المواقع الشبكيّة عن البرمجيات في حاسوبك، وتاريخ تثبيتها، والميزات التي فعلتها وما إلى ذلك. وفي

حـالات عدّة، تكفي تلك المعلومات كي يجري التعرّف بدقة إلى حاسـوبك[1] دون سواه.

صرنـا نتواصل باطراد مع العائلة والأصدقاء والمعارف وزملاء العمل بواسـطة الكومبيوتـرات، مسـتخدمين في ذلـك البريـد الإلكـتروني، والرسـائل النصيّـة، و«فيسـبوك» و«تويتر» و«إنسـتغرام» و«سـناب شـات» و«واتـس آب» وكل ما هو دارج الآن. المعلومـات نتـاج فرعي لهذه الاجتماعيـة عالية-التقنية. ولا تكتفي هذه النُظُم بنقل البيانات، بل تنشـئ أيضاً سـجلات للمعلومات عن مجريات تفاعلاتك مع الآخرين.

عندما تتمشـى في الخارج، فلربما لا يخطر ببالك أنك تنتج معلومات، لكن الحال أنك تنتجها فعليّاً. إذ يُجري هاتفك النقّال باسـتمرار حسـابات حول مكان وجوده، اسـتناداً إلى أبراج شـبكة الخَلَـوي القريبة منه. ليس الأمر أن شركـة الخَلَوي تكترث كثـيراً بمـكان وجـودك، لكنها تحتـاج إلى معرفـة مكان هاتفـك الخَلَوي كـي تحوّل المكالمات إليه.

بالطبـع، عندما تسـتخدم ذلك الهاتف فعليّـاً، فإنّك تنتج مزيـداً من المعلومات: الأرقـام التي اتصلت بها واتصلت بك، والرسـائل النصيّة التي أرسـلتها وتلقيتها، ومـدّة المكالمـات ومـا إلى ذلـك. إذا كان هاتفـك ذكياً، فهو حاسـوب أيضـاً، وكل تطبيقاتك تنتج معلومات حين تسـتخدمها -وحتى حين لا تستخدمها أحياناً. لربما احتـوى هاتفك تقنيّة «جـي بي إس»(GPS) (*) التي تنتج بيانات عن مكان وجودك، بدقّـة تفـوق حتى ما تعطيه أبراج شـبكة الخلوي. إذ تسـتطيع تقنية «جي بي إس» في هاتفك الذكي أن تحدّد موقعك بدقّة تتراوح بين 16 و27 قدماً (= بين 5.2 و8.23

(*) تختصر عبارة «النظام الشامل لتحديد المواقع جغرافيّاً». ويرتكز عمل الـ «جي بي إس» على الاتصال مع سلسلة أقمار اصطناعيّة تستطيع تحديد مواقع الأشياء على الكرة الأرضيّة كلها.

متراً)، فيما تصل المسافة عينها إلى قرابة 2000 قدم (= 610 متراً) بالنسبة لأبراج الخَلَوي.

اشتر شيئاً ما من متجر، وستُنتج مزيداً من المعلومات؛ إذ تمثّل آلة المحاسبة نوعاً من الكومبيوتر يتولى صنع سجل عمّا اشتريت، وتاريخ الشراء وزمنه. وتسري تلك المعلومات في شبكة الكومبيوتر الخاصة بالمتجر. وإذا لم تشتر بالمال نقداً، فلسوف تربط تلك المعلومات ببطاقتك الائتمانيّة. كذلك سترسل المعلومات إلى الشركة التي أعطتك تلك البطاقة، بل إن بعضاً من المعلومات سيظهر في قائمة حسابك الشهري فيها.

ربما احتوى المتجر أيضاً كاميرا فيديو للرقابة توضع بهدف تسجيل أدلة في حال حدوث فساد أو سرقة. وهناك كاميرا أخرى تصوّرك أثناء استخدامك آلة الصرّاف الآلي («إيه تي أم»/ ATM). وهناك كاميرات أخرى تراقب المباني والطُرُق وممرات المشاة والفضاءات العامة الأخرى.

اركب سيّارتك، وستولّد مزيداً من المعلومات، إذ باتت السيّارات الحديثة مكتظة بالحواسيب[2] التي تولّد معلومات عن سرعتك، وقوة ضغط قدمك على الدوّاسات، ووضعيّة المقود وما إليها. تتجمّع معظم تلك البيانات بصورة أوتوماتيكيّة في الصندوق الأسود للسيّارة[3]، الذي يفيد في معرفة ما حصل أثناء حادث ما. حتى عجلات السيارة يحتوي كل منها حاسوباً لقياس الضغط فيها. وعندما تأخذ سيّارتك إلى التصليح، فإنّ أول ما يفعله الميكانيكي هو الدخول إلى تلك المعلومات كلها كي يشخّص المشكلات. السيّارة ذاتيّة القيادة(*) تولّد 1 غيغابايت من البيانات في كل ثانية[4].

(*) يطلق التعبير على السيارات التي يقودها إنسان آلي (روبوت).

التقـط صورة، وسـتدخل في عملية إنتـاج المعلومات مجـدّداً؛ إذ تحتوي الكاميرا الرقميّة بيانات عن تاريخ التقاط الصورة وزمانها ومكانها[5]- نعم، تحتوي كاميرات عدّة تقنية «جي بي إس»- ومعلومات شاملة عن نوعها وعدساتها وإعداداتها، ورقم بطاقـة هويّـة الكامـيرا ذاتها. وعندمـا تضع الصورة عـلى الـ «ويـب»[6]، تبقى تلك البيانات مرتبطة بها.

لم تكـن الأمور دومـاً على ذلك النحو. في عصر الصحـف والراديو والتلفزيون، كنّـا نتلقـى المعلومـات دون وجود سـجل عنهـا، بينما نتلقـى الآن الأخبـار والمواد الترفيهيّـة بواسـطة الإنترنت. اعتدنـا طويلاً أن نتحدّث إلى النـاس وجهاً لوجه، ثم عـبر الهاتـف؛ فيما ينـوب البريد الإلكـتروني والمحادثات النصيّة عـن ذلك حاضراً. واعتدنا أن نشـتري الأشـياء نقداً من المتجـر، لكننا نسـتخدم الآن بطاقات الائتمان عبر شـبكة الإنترنت. واعتدنا أن نسـتعمل القطع النقدية المعدنيّة في إجراء مكالمات من كشك الهاتف، والمرور بالباب الدوّار لمترو الأنفاق، وتشغيل عدّاد رَكْن السيارة قرب الرصيف. الآن، نسـتخدم نُظُماً أوتوماتيكية للدفـع، مثل «إيزباس»(EZPass)[7]، مرتبطـة بأرقام لوحة السـيارة وبطاقـة الائتمان. كان الدفع لسـيارة الأجرة نقداً بصـورة حصريّـة في الماضي، ثم بدأنـا ندفع ببطاقـات الائتمان، وبتنا الآن نسـتخدم الهاتـف الذكـي للدخـول إلى نظـم شـبكات سـيارات الأجـرة كـ «أوبـر» (Uber) و«ليفت» (Lyft)، التي تصنع سـجلات للمعطيات عن تعاملاتها، إضافة إلى مواقع صعودنا إلى التاكسي ونزولنا منها. وباستثناءات قليلة محددة، توجد الحواسيب الآن في كل أماكن التعامل التجاري ومعظم أمكنة لقائنا مع أصدقائنا.

في السـنة الفائتة، حين تعطّلت ثلاجتي اسـتبدل رجـل التصليحات الكومبيوتر الـذي يديرهـا. أدركت حينهـا أنني كنت متخلّفـاً في نظرتي إلى الثلاجـة: إنّها لم تعد ثلاجـة بكومبيوتـر، بـل كومبيوتر يبقي عـلى الطعام بـارداً. وعلى غرار ذلـك تماماً، تتحول الأشـياء كلها إلى حواسـيب. هاتفـك كومبيوتر يجري مكالمات. وسـيارتك

حاسـوب بعجلات ومحرّك. وفرنك حاسـوب يخبز أطباق «اللاسانيه». وكاميرتك هـي كومبيوتـر يلتقط صوراً. حتى حيواناتنا المنزليّة ومواشـينا تُغـرس فيها رقاقات إلكترونيّة بصورة منتظمة: قطّتي عملياً كومبيوتر ينام في الشمس طيلة النهار.

كذلك صارت الكومبيوترات منبثّة في المزيد من أنواع السلع المرتبطة بالإنترنت. هناك شركة اسـمها «نسْـت» (Nest) اشـتراها محـرّك البحث «غوغـل» بما يزيد على 3 بليـون دولار في عـام 2014، تصنع آلة ذكيّة مرتبطـة بالإنترنت[8] لتنظيم حرارة المنـزل. وتعمل تلك الآلة على التأقلم مع عاداتك السـلوكيّة من جهة، وتتفاعل مع مـا يحدث مع شـبكة الكهرباء العامة من الجهة الثانيـة. ولتتمكن من إنجاز ذلك، لا تكتفي تلك الآلة بتسجيل مقدار ما تستهلكه من الكهرباء، بل تنشئ سجلاً ثابتاً عن حـرارة منزلك ورطوبته ومقدار الضوء المحيط، ومـا يتحرّك قربه أيضاً. وبإمكانك شراء ثلاجة ذكيّة تحتفظ بسجل عن تاريخ صلاحية الأطعمة[9]، ومكيّف هواء ذكي يرصـد تفضيلاتك كي يرفع كفـاءة الطاقة إلى حدّها الأقصى[10]. وهناك المزيد آتٍ: تبيع «نِسـت» الآن مجسّاً ذكيّاً[11] للدخان وثاني أوكسيد الكربون، وتخطّط لمجموعة كاملة من المجسّـات المنزليّة. كذلك تشـتغل مجموعة كبـيرة من الشركات على صنع مروحة واسـعة من الأدوات الذكيّة. وسيكون ذلك ضرورياً إذا أردنا نشر شبكات كهرباء ذكيّة[12] تستطيع خفض استهلاك الطاقة وانبعاث الغازات الدفيئة(*).

نبدأ جمع المعلومات وتحليلها حول أجسـادنا كوسـيلة لتحسين صحتنا وعافيتنا. عندمـا ترتـدي جهـاز تتبّـع اللياقـة البدنيـة، كـ«فيتبـت» (Fitbit) و«جوبـون» (Jawbone)، فإنّـه يجمـع بيانات عن تحرّكاتك أثناء اليقظة والنوم، ثم يسـتعملها في تحليـل عاداتك في التمرين والنوم، ويسـتطيع أن يحدّد متى تمـارس الجنس[13]. كلما أعطيـت ذلك الجهاز مزيداً من المعلومات عنك- كوزنك وغذائك- زادت إمكانية

(*) تشـير التسـمية إلى الغـازات التـي تلوثّ الغـلاف الجوي لـلأرض وتتسبّب في ظاهـرة الاحتباس الحراري.

معرفتك[14]. وبالطبع، تلك المعلومات التي تتشـارك بها مع جهازك موضوعة على الإنترنت.

تبدأ مجموعـة أدوات طبيّة بالتزوّد بالقدرة على دخول الإنترنت[15]، وهي تجمع مروحة من بيانات القياسات الحيوية، وتنشئ سجلات عنها. هناك للتو - أو سيكون هنـاك قريبـاً- أدوات تقيس باسـتمرار مؤشّراتنـا البيولوجيّة الأساسـيّة، وأحوالنا المزاجيّة ونشـاطات أدمغتنا. ولا يقتصر الأمر على الأدوات المختصّة[16]، بل تحتوي الهواتف الذكيّة الحالية بعض المجسّـات الحساسّـة لقيـاس الحركة. ومع الانخفاض المتواصل في سـعر تفكيك شـيفرة الحمض النـووي الوراثـي «دي إن إيه» (DNA)، يعمـد المزيـد منا إلى توليد المعلومـات وتحليلها عن جيناتنـا. وتأمل شركات كـ«23 أنـد مي» (23andMe)[17]، في اسـتعمال المعلومات عن جينـات زبائنها للتوصّل إلى تحديـد الجينات المتّصلـة بالمرض، ما يقود إلى صنع علاجـات مبتكرة ومربحة جداً. وتتحدث تلك الشركات عن التسويق المُشَخْصَن[18]، وربما تشتري شركات التأمين ذات يـوم ما جمعتـه تلك الشركات من معلومـات[19]، لتسـتخدمها في التوصّل إلى قرارات بشأن عملها.

لربـما تتمثّـل الصورة القصوى لمسـار التوليد الذاتي للمعلومات في صنع سـجل لحيـاة الفـرد[20] يعمل على التجميـع المتواصل للمعلومات الشـخصيّة. تتوافر للتو تطبيقات لصنع سجل حياة الفرد يمكنها تسجيل نشاطاتك على هاتفك الذكي، مثل الأوقـات التـي تتحدث بها مع أصدقائك، أو تمارس الألعـاب الرياضيّة، أو تذهب إلى السـينما وغيرها. لكن ذلك لا يمثل سـوى ظل باهت عما سوف تكونه سجلات الحياة. سـوف تضم تلـك التطبيقات مسـتقبلاً سـجلاً بالفيديـو[21]. وتعتبر نظارة «غوغـل» أول أداة تقنيّـة قابلـة للارتداء تقدر على صنع سـجل حيـاة بالفيديو[22]، لكنّ هنالك عديدين يسعون للحاق بها.

هـذه أمثلـة عـن «إنترنـت الأشـياء» (Internet of Things)[23]. سـوف ترصـد مجسّـات بيئية مسـتويات التلوث. وسـتعمل نُظُم التحكّم وقوائم الجرد الذكيّة على خفـض الهدر وتوفير المال. وسـوف تدخـل كومبيوترات متّصلـة بالإنترنت في ثنايا الأشياء كافة - فيكون لدينا مدن ذكية[24]، وفراشي أسنان ذكية[25]، ومصابيح إنارة كهربائيّـة ذكية[26]، وأرصفة طرق ذكية[27]، وزجاجـات أدوية ذكية[28]، وملابس ذكيّـة[29]- ولِمَ لا؟[30] تشـير التقديـرات حاليـاً إلى وجود 10 بلايـين جهاز متّصل بالإنترنـت[31]. ويفـوق الرقـم للتو عدد سـكان كوكب الأرض، بـل إنني طالعتُ تقديـرات تتوقع وصول الرقم إلى 30 بليوناً في العام 2020. مسـتوى النشـاط[32] مرتفـع جـداً في هذا المجال، ولا نعرف الآن أي التطبيقات سـيعمل وأيّها سيفشـل. ما نعرفه تماماً أننا جميعاً سنسـتمر في توليـد معلومات، كميات هائلة من المعلومات. وسوف تضحي كل الأشياء التي تحيط بنا عيوناً وآذاناً للإنترنت[33].

تأثـيرات كل هذه الاتّصالية الشـاملة على الخصوصية عميقة. كل تلك الأدوات الذكيّة ستخفض انبعاثات الغازات الدفيئة -لكنها ستضخّ أيضاً سيلاً من المعلومات عـن النـاس وتحركاتهم في منازلهم وكيف يقضون أوقاتهم. وسـوف تجمع إشـارات السير الذكيّة معلومات عن تحرّكات الناس خارج بيوتهم[34]. لن تصبح الكاميرات إلا أفضـل وأصغـر وأكثر تحرّكاً[35]. شركـة «ريثيـون» (Raytheon)(*) تعتزم وضع منطـاد صغـير في سـماء مدينتي واشـنطن العاصمـة وبالتيمور في عـام 2015 [36]؛ لاختبار قدرتها على تتبّع «أهداف»- يفترض أنها عربات- في البر والبحر والجو.

في المحصلـة، نحن نتفاعل مع مئات الكومبيوترات يوميّاً، وسرعان ما سـيرتفع عددهـا إلى الآلاف. كل واحـد من هـذه الكومبيوتـرات ينتج معلومـات، والقليل منهـا من النوع المثمر: ما طلبناه في مطعم، أو معدل دقّات قلبنا في هرولة المسـاء، أو

(*) تنـدرج شركـة "ريثيـون" ضمـن الـشركات السـبع الكـبرى المختصـة في صنـع الأسـلحة للجيش الأميركي.

آخر رسالة حبّ كتبناها. في المقابل، يندرج معظم تلك المعلومات ضمن ما يسمّى «ميتاداتا» أو بيانات حول البيانات («بيانات وصفيّة»/ Metadata). والبيانات حول البيانات معلومات يستخدمها نظام كومبيوتر كي يعمل، أو معلومات تكون منتجاً جانبياً لعمل الحاسوب. في نظام رسائل نصيّة، تعدُّ الرسائل نفسها معلومات، لكن الحسابات التي أرسلت الرسائل وتلقتها، إضافة إلى زمنها وتوقيتها، هي كلها «بيانات وصفيّة» أو «ميتاداتا». يعمل نظام البريد الإلكتروني[37] على نحو مماثل، إذ تعدُّ نصوص البريد الإلكتروني معلومات، لكن المعلومات عن المُرسِل والمتلقي ومسار الرسائل وأحجامها «ميتا داتا»- ويمكن الجدل حول كيفية تصنيف سطر المحتوى. في الصورة الفوتوغرافية، الصورة ذاتها معلومات؛ لكن تواريخها والرقم المتسلسل للكاميرا، ومعطيات إعداداتها، ومعلومات الـ «جي بي إس» عنها، هي ـ «ميتاداتا». قد تبدو الـ «ميتا داتا» غير مهمة، لكنها ليست كذلك البتة، وفق ما سأظهره لاحقاً.

استطراداً، لا تنجم تلك الغيوم من المعلومات التي ننتجها بالضرورة عن خداع ومراوغة أي طرف. إذ يأتي معظمها ببساطة كمنتج جانبي طبيعي لعمل الحواسيب. هكذا تعمل التكنولوجيا حاضراً. البيانات هي «دخان عوادم»(*) عصر المعلومات.

ما هي كميّة المعلومات؟

إليك بعض الحسابات السريعة. ربما تكون سعة القرص الصلب في كومبيوترك المحمول 500 غيغابايت (Gigabyte). ولعلك اشتريت قرصاً صلباً احتياطيّاً لتخزين المعلومات بسعة 2-3 تيرابايت (Terabyte). وربما يكون القرص الصلب في الشبكة الداخلية لشركتك أكبر ألف مرّة من ذلك، أي بيتابايت (Petabyte). هنالك أسماء للأرقام الأكبر. إذ إن كل ألف بيتابايت تسمّى إكزابايت (Exabyte)[38]،

(*) يشير التشبيه إلى الدخان الذي يصدر عن عوادم السيارات.

وهي تساوي بليون بليون بايت؛ وكل ألف إكزابايت تسمّى زيتابايت (Zettabyte)، وكل ألف زيتابايت اسمها يوتابايت (Yottabyte). بتعابير بشريّة، كل إكزابايت من المعلومات تساوي خمسمائة بليون صفحة من النصوص.

يتجمع «دخان عوادم» المعلومات مع بعضه بعضاً. بحلول عام 2010، كنّا كجنس بشري ننتج من المعلومات في اليوم الواحد أكثر مما أنتجناه منذ بداية الزمن حتى عام 2003[39]. وبحلول عام 2015، بات 76 إكزابايت من المعلومات تنقل عبر الإنترنت سنوياً[40].

عندما نبدأ التفكير بتلك المعلومات كلها، يبدو من السهل صرف النظر عن الانشغالات بشأن الاحتفاظ بها واستعمالها، بناء على الافتراض بأن كميّات المعلومات ببساطة أكبر من القدرة على تخزينها؛ وأن وفرتها الكبيرة في كل الأحوال تجعل من الصعب «غربلتها» للعثور على شذرات معلومات مفيدة. كان ذلك صحيحاً في الماضي. ففي مطالع العصر المعلوماتي، جرت العادة على التخلّص من معظم تلك المعلومات - معظم «البيانات الوصفيّة» بالتأكيد- بعد وقت قصير من صنعها. بدا حينها أن تخزين تلك المعلومات يستلزم مساحات كبيرة من الذاكرة. لكن تكلفة مناحي الحوسبة كافة، انخفض بصورة مطردة مع مرور السنين، وما كان ينظر إليه قبل عقد بوصفه كميّات معلومات ليس من العملي تخزينها ومعالجتها، صار أمراً يسهل التعامل معه اليوم. في العام 2015، بلغت تكلفة تخزين 1 بيتابايت من المعلومات في سحابة رقميّة، قرابة مئة ألف دولار سنوياً[41]، ما يمثّل هبوطاً بقرابة 90 ٪ عن المليون دولار التي كانت كلفة تخزينها في عام 2011. النتيجة تخزين المزيد والمزيد من المعلومات.

الأرجح أنك تستطيع تخزين كل تغريدة أرسلتها يوماً من محرك أقراص كومبيوترك المنزلي[42]. فتخزين المكالمات الصوتية من هواتف الولايات المتحدة

كافـة[43] يسـتلزم أقـل مـن 300 بيتابايـت، أو تكلفـة 30 مليون دولار في السـنة. ويتطلّـب تخزين سـجل الحياة الشـخصيّة في شريط فيديـو 700 غيغابايت للفرد في السـنة. إذا ضربت ذلك بعدد سـكان الولايات المتّحدة، يصل الرقم إلى 2 إكزابايت سـنويّاً، بتكلفـة حالية تبلغ 200 مليـون دولار. هذا مكلف، لكنـه في متناول اليد، والسـعر سـينخفض باسـتمرار. في العام 2013، أكملـت «وكالة الأمـن القومي» تشـييد قاعدتها الضخمة، «مركز يوتا للمعلومـات» (Utah Data Center) في مدينة بلَفديـل، وهـو حاليا ثالث أكـبر مركز معلومـات في العالم[44]، والأولُ في سلسـلة مراكز تبنيهـا «وكالة الأمن القومي». التفاصيل سرية[45]، لكن الخبراء يعتقدون أنّ «مركز يوتا» يسـتطيع تخزين 12 إكزابايت من المعلومات، وبلغت تكلفته حتى الآن 1.4 بليون دولار[46]. على الصعيد العالمي، تسـتطيع مؤسّسـة «غوغل» تخزين 15 إكزابايت[47].

ما يصح على المؤسّسات ينطبق على الأفراد أيضاً، وأنا نفسي مثال وحالة للدراسة. إذ يمتد تاريخ بريدي الإلكتروني إلى العام 1993، واعتبر ذلك الأرشـيف البريدي جزءاً من دماغي. إنّه ذكرياتي. لا يمر أسبوع دون أن أقلّب ذلك الأرشيف بحثاً عن شيء ما: مطعم زرته قبل سنوات، مقال أخبرني أحدهم عنه، اسم شخص ما قابلته. وأنا أرسـل إلى نفسي رسـائل تذكيريّة عبر الـ «إيميل» طيلة الوقت؛ لا يقتصر أمرها على أشـياء يجب أن أنجزها عند عودتي إلى المنزل، بل أيضاً تذكيرات بأشـياء قد أود استرجاعها بعد سنوات مستقبلاً. الوصول إلى ذلك المخزن وصول إلي كشخص.

اعتـدت أن أفـرز ذلـك البريـد بانتباه تـام. يجب عـليّ أن أقرّر ما يجـب حذفه أو الاحتفـاظ بـه، وأعمـد إلى إضافة الرسـائل التي أقـرّر تخزينها مع مئـات غيرها، في ملفات مصنّفة وفق أسـماء الأشخاص، والشركات، والمشاريع، وهكذا دواليك. في العـام 2006، توقّفت عن فعل ذلك، وأخزّن الرسـائل كلها حالياً في ملف ضخم، فمنذ عام 2006، صار التخزين والبحث بالنسبة لي أسهل من الفرز والحذف.

مـن أجل فهم ما يعنيه ركـم كل تلك المعلومات للخصوصيّة الشـخصيّة، يجدر التفكـير بطالب الحقوق النمسـاوي ماكس شريمز. في العـام 2011، طلب شريمز مـن موقع «فيسـبوك» أن يعطيه كل مـا يملكه من معلومات عنه[48]. واسـتند طلبه إلى قوانـين «الاتّحـاد الأوروبي». وبعـد سـنتين، وعقـب منازعة في المحاكم، أرسـل «فيسـبوك» إلى شريمز أسـطوانة مدمجة («سي دي» / CD) تضم 1200 ملفاً من نوع «بي دي أف/ pdf» [49]. لم تقتـصر محتويات الـ «سي دي» على كل الأصدقاء الذين يعرفهـم، والأخبار التـي تتبّعها، بل ضمّت أيضاً كل الصـور والصفحات التي نقر عليهـا، وكل الإعلانـات التي رآها. شركة «فيسـبوك» لا تسـتخدم تلك المعلومات كلهـا، لكـن بـدل أن تفرزها وتقـرّر ما يجب الاحتفـاظ به، وجـدت الشركة أن من الأسهل الاحتفاظ بكل شيء.

2

المعلومات بوصفها رقابة

تعمل الحكومات والشركات معاً على تجميع المعلومات التي تنهمر منا في خضم حياتنا الرقميّة وتخزينها وتحليلها. يجري ذلك غالباً من دون معرفة منا، ومن دون طلب موافقتنا. واستناداً إلى تلك المعلومات، تتوصّل الحكومات والشركات إلى استنتاجات بشأننا، ربما لا نوافق عليها، أو حتى نحتج ضدّها؛ لكنها تؤثّر في حياتنا بطريقة عميقة. قد لا نحب أن نعترف بذلك، لكننا بتنا نعيش تحت رقابة واسعة.

يأتي كثير مما نعرفه عن «وكالة الأمن القومي»[1] من إدوارد سنودن، على الرغم من أنّ أشخاصاً عديدين، قبل سنودن وبعده، سرّبوا أسراراً عن الوكالة. وبوصفه متعاقداً مع «وكالة الأمن القومي»، جمع سنودن عشرات الآلاف من الوثائق تتضمن توصيفاً لنشاطات رقابيّة تمارسها. وفي عام 2013 فرّ سنودن إلى هونغ كونغ، وأعطى وثائق لصحافيّين انتقاهم بنفسه. لفترة من الزمن، عملتُ مع غلين غرينوالد وصحيفة الغارديان البريطانيّة على تحليل وثائق من سنودن غلب عليها الطابع التقني.

برزت الأخبار الأولى عن مسألة سنودن متضمّنة وصفاً للطريقة التي دأبت بها «وكالة الأمن القومي» على جمع بيانات عن سجلات مكالمات الأميركيين الخَلَوية[2]. إحدى الحجج التي دافعت بها الحكومة عن نفسها في نبرة تكرّرت كثيراً في أوقات لاحقة[3]، تمثّلت في القول إنّ ما جمعته الوكالة كان مجرد «بيانات وصفيّة». تسعى

تلك الحجة إلى القول إن الوكالة لا تجمع الكلمات التي نقولها لبعضنا بعضاً بواسطة الخلوي[4]، بل تكتفي بالبيانات عن أرقام الهواتف، وتاريخ المكالمات، وتوقيتها ومدّتها. بدا أن ذلك قمين بتهدئة الناس، لكن الأمور لم تجر على ذلك النحو. الحال أن جمع الـ «ميتاداتا» عن الناس يعني وضعهم تحت الرقابة[5].

يمكن إقامة البرهان على بطلان تلك الحجة بواسطة تدريب ذهني بسيط. تخيّل أنك استأجرت مخبراً خاصاً كي يتنصّت على شخص ما. سوف يزرع المخبر لواقط سريّة في منزل ذلك الشخص، ومكتبه، وسيارته. سوف يتنصّت أيضاً على هاتف ذلك الشخص وكومبيوتره. وسوف يزوّدك بتقرير عن مكالماته.

تخيّل الآن أنّك طلبت من المخبر وضع ذلك الشخص تحت الرقابة. سوف تحصل على تقرير مختلف لكنه يبقى شاملاً إذ يضمّ الأمكنة التي يتردّد عليها ذلك الشخص، وما الذي يفعله، وما هي مشترياته. تلك هي «البيانات الوصفيّة».

إذاً، التنصّت يوصلك إلى كلام المحادثات الهاتفية، أما الرقابة فتعطيك كل شيء آخر.

تكشف «البيانات الوصفيّة» للهواتف وحدها أشياء كثيرة عنا. إذ تظهر مدّة المكالمات وتكرارها وأوقاتها علاقاتنا مع الآخرين: أصدقاءنا الحميمين، وزملاء العمل، وكل من يقع بين هاتين الفئتين. وتتكفل «البيانات الوصفيّة» للهواتف[6] بكشف من هم الأشخاص الذين نهتم بأمرهم، وطُرُق اهتمامنا بهم، وما هي الأشياء التي نعتبرها مهمة، مهما كانت خصوصيّتها. تفتح تلك المعلومات نافذة تطل على شخصياتنا[7]، وتقدّم ملخّصاً تفصيليّاً عن ما يحصل معنا في الأوقات كلّها[8].

في تجربة أجرتها «جامعة ستانفورد»، جرى تجميع «البيانات الوصفيّة» لهواتف 500 متطوّع على مدار بضعة شهور. وتفاجأ حتى الخبراء أنفسهم بمدى الطابع الشخصي الذي استطاعوا بلوغه في استنتاجاتهم المستندة إلى «ميتاداتا» هواتف المشاركين[9]. يستأهل التقرير عن تلك التجربة الاقتباس:

- اتّصل المشارك (أ) بمجموعات محليّة مهتمة بالأمراض العصبيّة، وبصيدليّة مختصة، وبخدمة رعاية مرض نادر، وبـ «خط ساخن» مع شركة أدوية مختصة حصريّاً بعلاج مرض «التصلّب اللويحي المتعدّد» (Multiple Sclerosis) والمرتكس.
- تحدّث المشارك (ب) طويلاً مع مختصّين في أمراض القلب يعملون في مركز طبي كبير، وتحدّث باقتضاب مع مختبر طبي، وتلقى مكالمات من صيدلية، وأجرى مكالمات قصيرة مع «خط ساخن» لمركز يقدم تقارير عن جهاز طبي يستعمل لرصد «اضطرابات نبضات القلب».
- أجرى المشارك (ت) عدداً من المكالمات مع متجر لبيع الأسلحة مختص بتجارة البنادق نصف الآلية من نوع «إيه آر»، كما تحدّث طويلاً مع مركز خدمة الزبائن لأحد منتجي تلك البنادق.
- اتصل المشارك (ث) على امتداد ثلاثة أسابيع مع محل لتصليحات المنازل، وصانع أقفال، ومركز مختص بالزراعات المائيّة(*)، ومتجر لبيع أدوات تستعمل في تعاطي مواد الكيف.
- أجرت المشاركة (ج) اتّصالاً صباحيّاً طويلاً مع أختها. وأجرت بعد يومين سلسلة مكالمات مع موقع محلي لتنظيم الأسرة، ثم أجرت اتصالات أخرى قصيرة بعد أسبوعين، واتصالاً أخيراً بعد شهر.

استناداً إلى خط «بيانات وصفيّة» واحد، خلص الباحثون إلى أن المشاركين كانوا على التوالي: مريضاً يعاني «التصلّب اللويحي المتعـدد»، ومصاباً بنوبة قلبية، ومالك بندقية حربيّة نصف آلية، وزارعاً منزلياً لحشيشة الكيف، وامرأة أجرت إجهاضاً.

(*) زراعة منزلية غالباً لا يستعمل فيها التراب.

تعدُّ عمليات البحث عن المعلومات على الإنترنت مصدراً آخر للمعلومات الحميمة التي يمكن استعمالها في الرقابة[10]. (تستطيع المجادلة طويلاً إن كانت تلك بيانات أم «بيانات وصفيّة». تزعم «وكالة الأمن القومي» أن تلك البيانات هي «ميتاداتا»[11]؛ لأن مكوّنات البحث متضمّنة في روابط إلكترونيّة ضمن صفحات الإنترنت ومواقعها). نحن لا نكذب على محرّك البحث، إذ تربطنا به علاقة أشد حميميّة من تلك التي تربطنا بأصدقائنا، وأحبتنا، وأفراد عائلتنا. ونحن دوماً نخبره بما نفكّر، وبأوضح ما يمكن من كلمات. يعرف «غوغل» جيّداً نوع الـ «بورنو» الجنسيّ الذي يبحث عنه كل منا، وأيّاً من الأحبة القدماء ما زال في بالنا، وما نخجل منه، وما نهجس به، وما نبقيه سراً. إذا عقد «غوغل» العزم، فبإمكانه أن يعرف أيّاً منا قلقٌ على صحته العقليّة-النفسيّة، أو مهتمٌّ بالتهرب من الضرائب، أو يخطط للاحتجاج ضد سياسة حكومية معيّنة. اعتدتُ القول إنّ «غوغل» يعرف ما أفكر به أكثر من زوجتي، لكن ذلك لا يذهب بعيداً بما يكفي، فـ «غوغل» يعرف ما أفكر به أكثر مما *أعرف أنا*؛ لأنّه يتذكر الأشياء كلها بوضوح وإلى الأبد.

أجريت تجربة سريعة لخاصيّة الاستكمال التلقائي في محرّك البحث «غوغل». وتمنح تلك الخاصيّة إمكان أن يستكمل «غوغل» في الزمن الحقيقي ما بدأت كتابته في خانة البحث، استناداً إلى ما كتبه آخرون في السابق. عندما كتبت: «هل يجب أن أخبر (w) (*)...»[12]، استكمل «غوغل» العبارة، فكتب: «هل يجب أن أخبر زوجتي أني أقمت علاقة غرامية»؟ و«هل يجب أن أخبر عملي حول قيادتي السيارة تحت تأثير (الكحول أو المخدرات)»؟ كتب «غوغل» ذلك لأنها العبارتان الأكثر شيوعاً بين جمهور مستخدميه. و«غوغل» يعرف كل الأشخاص الذين نقروا على استكمال إحدى العبارتين، إضافة إلى كل الأشياء الأخرى التي بحثوا عنها يوماً[13].

(*) قد يشير حرف (w) بالإنكليزية إلى الحرف الأول في كلمة زوجة (wife) أو عمل (work)، ولذلك اختار برنامج الاستكمال التلقائي الإجابتين الواردتين في المثال.

في عــام 2010 اعترف إريك شـميدت، المديـر التنفيذي لـ «غوغـل»[14]، بأننا «نعرف أين أنت، ونعرف أين كنت، ويمكننا أن نعرف تقريباً ما تفكر به».

إذا كان لديـك حســابٌ في البريد الإلكـتروني «جي ميـل» (G– Mail)، يمكنك أن تتأكّـد مـن الأمر بنفسـك. إذ تسـتطيع أن تعرف الأوقات التـي دخلت فيها على ذلك البريد، منذ لحظة إنشــائك حســابك عليه، وربما لسـنوات طويلة. افعل ذلك، وسـوف تصاب بالدهشة. إنّه أشـد حميميّة مما لو كنت أرسلت لـ«غوغل» مفكرتك الشـخصيّة. وعلى الرغم من أن «غوغل» يتيح لك التحكّم بالإعلانات التي ترغب في مشـاهدتها، فأنـت لا تملـك الحق في حذف أي شيء لا ترغب به على حسـابك في «جي ميل».

ثمة مصادر أخرى للمعلومات الحميمة و«البيانات الوصفيّة». فالسـجلات عن عاداتك في التسـوّق تستطيع أن تكشف أشـياء كثيرة عمن تكون. وتعلن تغريداتك عـلى «تويـتر» للعـالم موعـد اسـتيقاظك صباحـاً[15]، وموعـد إيوائـك إلى الفراش ليـلاً. كما تكشـف لوائح أصدقائك عن ميولك السياسـيّة وخياراتك الجنسـيّة[16]. وتخبر عناوين رسـائل بريـدك الإلكتروني عمن يحتل مركز القلـب في حياتك المهنيّة والاجتماعيّة والعاطفيّة[17].

إحـدى الطرق للتفكير في تلك المواضيع تتمثّل في النظر إلى المعلومات باعتبارها محتـوى، فيما «البيانـات الوصفيّة» هي سـياق ذلك المحتوى. تسـتطيع الـ «ميتاداتا» أن تكشـف أكثر مما تفعله المعلومات نفسـها، خصوصاً إذا جُمِعـت وصُنِّفَت. عندما تضع شـخصاً تحت الرقابة، تفوق أهمية محتويات المكالمات الهاتفيّة والرسائل النصيّة والبريـد الإلكـتروني ما تمتلكـه «البيانـات الوصفيّة». لكـن، عندما تفـرض الرقابة العامة، تكون الـ «ميتاداتا» هي الأكثر دلالة وأهميّة وفائدة[18].

كما قال ستيوارت بيكر، المستشار العام السابق لوكالة الأمن القومي، من المؤكّد أنّه «باستطاعة «البيانات الوصفيّة» أن تخبرك كل شيء تماماً عن حياة شخص ما[19].

إذا كان لديـك ما يكفي مـن الـ «ميتاداتا»، فأنت لا تحتاج عمليّـاً إلى المحتوى»[20]. وفي 2014، علّـق مايكل هايدن، المدير السـابق لـ «وكالـة الأمن القومي» و«وكالة الاستخبارات المركزية» (CIA) قائلاً: نحن نقتل الناس اعتماداً على الـ«ميتاداتا»[21].

الحقيقـة أن الفـارق بـين المعلومـات و«البيانـات الوصفيّة» وهمـي إلى حدّ كبير؛ فكلاهما معلومات عنّا.

رقابة أرخص

تاريخيّاً، كانت الرقابة صعبة ومكلفة. كنا نلجأ إليها فقط حين يكون الأمر مهماً: عندمـا تحتـاج الشرطة لتعقب مشـتبه فيـه، أو عندما تبحث شركة تجاريـة معيّنة عن سجل مفصل لتاريخ المشتريات لأغراض تتعلق بفواتيرها. كان هنالك استثناءات، وهـي متطرّفـة ومكلفـة. حكومـة ألمانيـا الشرقيّة المريضـة إلى حد اسـتثنائي بجنون الارتياب جنّدت 102 ألف شـخص في صفوف جهاز الاسـتخبارات «سـتازي»، لمراقبـة مجمـوع السـكان البالـغ 17 مليـون نسـمة، بمعـدل جاسـوس لـكل 166 مواطناً[22]، أو جاسوس لكل 66 مواطناً إذا أضفت إلى الحساب المخبرين المدنيين.

تطـوّرت رقابـة الشركات مـن جمع القليل الـضروري إلى جمع كل مـا يمكن من المعلومـات. في المـاضي كانت الشركات دائـماً تجمع معلومات عـن زبائنها، لكنها لم تجمـع الكثـير منها، واحتفظت بها بمقـدار ما كان ذلك ضروريّـاً. شركات بطاقات الائتـمان كانـت تجمـع المعلومات فقـط عن معامـلات زبائنهـا الماليّة التـي تحتاجها لأغـراض الفواتـير. والمتاجـر بالـكاد جمعـت معلومـات عـن زبائنها، فيـما لم تجمع شركات شـحن البضائع بالبريد سـوى الأسماء والعناوين، وربما مع شيء من تاريخ المشـتريات كي تعرف متى ترفع اسـم أحدهم من قوائمهـا البريدية. حتى «غوغل» عند بداياته الأولى، لم يجمع سـوى القليل من البيانات عن مسـتخدميه، بالمقارنة مع ما يملكه منها اليوم. عندما كانت معلومات الرقابة مكلفة الجمع والتخزين، اكتفت الشركات بأقل ما يمكن منها.

انخفضت تكلفة تقنيّات الحوسبة بصورة سريعة في العقود الأخيرة. كان ذلك أمراً جيداً إلى حد بعيد. أصبح من الأرخص والأسهل للناس التواصل ونشر أفكارهم والوصول إلى المعلومات وما إلى ذلك. لكن، في الآن ذاته، انخفضت تكلفة الرقابة. ومع التحسّن المطرد في تقنيّات الكومبيوتر، صار بمقدور الشركات جمع المزيد من المعلومات عن كل من تتعامل معه. ومع انخفاض تكاليف تخزين المعلومات، استطاعت الشركات حفظ المزيد من المعلومات لزمن أطول. وإذ صارت أدوات تحليل البيانات الضخمة أشد قوّة، بات تجميع مزيد من المعلومات أمراً مجزياً تماماً. أدى ذلك إلى ظهور نماذج الأعمال المستندة إلى الرقابة، على نحو ما سأتحدث عنه في الفصل الرابع.

انتقلت رقابة الحكومة من العمل على جمع المعلومات عن أقل عدد ضروري من الأشخاص، إلى تجميعها عن أقصى عدد ممكن منهم. عندما كانت الرقابة يدويّة ومكلفة، كان من الممكن تبريرها في الحالات القصوى وحدها. فضرورة الحصول على مذكرة تفتيش قلصت رقابة الشرطة، كذلك عملت محدودية الموارد ومخاطر الانكشاف على تقليص رقابة الاستخبارات على مستوى الدولة. استهدفت الرقابة أشخاصاً بعينهم، وجمعت أقصى المعلومات عنهم وحدهم. كما وُجِدَت قوانين صارمة تقلّص إلى أدنى الحدود إمكان جمع المعلومات عن الآخرين. على سبيل المثال، عندما كان «مكتب التحقيقات الفيدراليّة» (إف بي آي/ FBI)(*) يترصّد هاتف أحد رجال العصابات، كان يفترض بمسترق السمع وقف التسجيل وإغلاق السماعة فوراً عندما يدخل على الخط أولاد الشخص أو زوجته.

مع تطوّر التقنية وانخفاض تكلفتها، وسّعت الحكومات نطاق الرقابة. تستطيع «وكالة الأمن القومي» الآن أن تراقب مجموعات كبيرة- الحكومة الروسية، والطواقم الدبلوماسيّة الصينيّة، والمنظّمات السياسيّة اليساريّة ونشطاءها- وليس مجرد أفراد.

(*) يتولى مكتب التحقيقات الفيدرالي ("إف بي آي") شؤون الاستخبارات الداخلية في أميركا.

وتعني إمكانيّة مراقبة المكالمات الصادرة عن الهواتف الجوالة إعطاء الـ «إف بي آي» قدرة التنصّت على الناس[23] بغض النظر عن الجهاز الذي يستعملونه في التواصل. وبالنتيجة، تستطيع وكالات الاستخبارات الأميركيّة التجسّس على شعوب بأكملها، وتخزين بيانات عنها لسنوات طويلة. وترافق ذلك مع تغيير في طبيعة التهديد، فقد استمرت تلك الوكالات في التجسّس على حكومات معيّنة، فيما وسّعت رقابتها الشاملة على مجاميع عريضة بحثاً عن أفراد يحتمل أن يكونوا خطيرين، وسأتحدّث عن ذلك في الفصل الخامس.

نتيجة لذلك، تلاقت مصالح الرقابة لدى الحكومات والشركات معاً. إذ بات كلاهما راغباً في معرفة كل شيء عن كل شخص. تتباين دوافع الطرفين[24]، لكن المنهجيّات نفسها، وهو السبب الرئيس للشراكة الأمنيّة القوية بين القطاعين الحكومي والخاص، التي سأتناولها في الفصل السادس.

لمعرفة ما أقصده بتكلفة تكنولوجيا الرقابة، يكفي النظر إلى أدوات التجسّس المتقدمة والرخيصة التي يحصل عليها الزبائن العاديّون. فأثناء رحلة جويّة، رُحتُ أقلّب صفحات مجلة سكاي مول (Sky Mall)، وهي «دليل سلع» تحرص الخطوط الجويّة على وضعه في خلفية مقاعد المسافرين في الرحلات الجويّة المحليّة في أميركا. لقاء 80 دولاراً، هناك قلم مع كاميرا خفيّة ومايكروفون، يمكّنني من تسجيل وقائع أي اجتماع أرغب في الإبقاء على دلائل عنه لاحقاً. وبإمكاني أن أشتري كاميرا خفيّة مثبّتة في راديو- ساعة، لقاء 100 دولار، أو كاميرا تعلق على حائط الغرفة على هيئة مستشعر للحركة. وأستطيع أن أضبط الكاميرتين كي تسجّلا ما يجري في الغرفة بصورة متواصلة، أو عندما تستشعران حركة فيها. وتتيح لي أداة أخرى الوصول إلى البيانات في الهواتف[25]- سواء أكانت «آي فون» (iPhone) أو «آندرويد» (Android)- بمجرد أن تكون في متناولي فعليّاً. ويوضح الإعلان عن تلك الأداة أنها تمكّن من «قراءة الرسائل النصيّة حتى بعد حذفها. ورؤية الصور، ولوائح الاتّصال، وتواريخ المكالمات، ومواعيد الروزنامة، والمواقع الإلكترونية

التي جرى الدخـول إليها، وحتى الدخول إلى بيانات تحديد المواقع جغرافيا (GPS) في الهاتف لمعرفة الأماكن التي زارها». ولا يتجاوز السعر 120 دولاراً.

من محلات أخرى، أستطيع بأقل من 50 دولاراً شراء مسجّل لوحة المفاتيح[26]، أو مسـجّل المفاتيـح، لمعرفـة ما يطبعه شـخص على لوحـة مفاتيح حاسـوبه بمجرد وصلـه مبـاشرة بالكومبيوتـر. ومقابـل قرابـة 100 دولار، أسـتطيع الحصـول على برنامـج يمكننـي مـن اعـتراض مكالمـة هاتفيّـة لشـخص قريـب منـي، والتنصّت عليهـا[27]. كذلك أسـتطيع بأقل من ألـف دولار شراء طائـرة «درون- هليكوبتر» تحمل كاميرا[28] ويمكن التحكّم بها عن بُعد، كي أتجسّس على جيراني.

إنّ الأدوات التـي ذكرتها في متناول المسـتهلك، على الرغم من أن بعضها محظور في بعـض الدوائر القانونية. كذلـك تتجه أدوات الرقابة المحترفة لأن تكون أرخص سـعراً وأكثر تطـوّراً[29]. بالنسـبة للشرطـة، يغيّر انخفـاض الأسـعار كل شيء. إذ يكلّف تتبع شـخص ما خفيّة، سـواء سيراً على الأقدام أم بالسيارة، قرابة 175 ألف دولار شـهريّاً -معظمها رواتب للعملاء القائمين بعملية التتبع. لكن، إذا اسـتطاع رجـال الشرطة دسّ متتبّع إلكتروني في سـيارة المشـتبه فيه، أو اسـتخدام برج زائف لاتّصالات الخلوي بهدف مخادعة هاتف المشـتبه فيه كي يرسل «المعلومات المكانيّة» إلى الشرطـة مبـاشرة، تنخفض تكلفة الملاحقـة إلى 70 ألف دولار شـهريّاً؛ لأنها لا تتطلّـب سـوى عميل واحـد. وإذا اسـتطاعت الشرطة أن تخبئ مسـتقبِل إشـارات الـ «جي بي إس» في سـيارة المشتبه فيه، تنخفض التكلفة فجأة إلى قرابة 150 دولاراً في الشـهر، معظمها تكلفة دسّ تلك الأداة خلسـة في السيارة. ويفوق تلك الوسائل كلها رخصاً الحصول على معلومات عن أمكنة المشـتبه فيه من مزود هاتفه الخلوي، وشركة «سبرينغ» (Spring) تقدّم تلك البيانات لقاء 30 دولاراً شهرياً.

يكمـن الفـارق بـين التكاليـف الثابتـة والهامشـيّة. إذا قـام قسـم شرطـة برقابة مباشرة[30] سـيراً على الأقدام سـتكون تكلفة تتبع شـخصين ضعفي رقابة شـخص

واحـد. لكـن الرقابة بواسـطة الخلوي أو نظـام الـ «جي بي إس»، تكلّف أساسـاً ما يسـتلزمه تثبيـت النظـام، وحالما يتم ذلك يصبح الفارق هامشـيّاً وضئيـلاً بين رقابة شخص واحد أو عشرة أشخاص أو ألف شخص. على نحو مماثل، بعد الإنفاق على تصميـم وبناء نظام تنصّت على الهواتف يجمع الأصوات ويحلّلها في أفغانسـتان، كما فعلت «وكالة الأمن القومي» للمسـاعدة في حماية الجنود الأميركيّين من المتفجّرات محليّة الصنع، يصبح من السـهل وبسـعر زهيد توظيف النظام التقني عينه للتنصّت على شبكات الهواتف في بلدان أخرى.

الرقابة العامة

لا يؤدّي الانخفاض المستمر في تكلفة تقنيّات الرقابة إلى مجرد فارق في السعر، بل إلى فـارق نوعـيّ أيضاً. إذ ينتهي الأمر بالمنظّمات إلى ممارسـة رقابة أكبر- أكبر بكثير. عقـب قـرار من «المحكمـة العليـا» الأميركيّة عـام 2012، مثلاً، طُلِـبَ من مكتب التحقيقـات الفيـدرالي الحصـول عـلى مذكـرات قضائيّة بشـأن 3 آلاف جهـاز تتبّع بواسـطة الـ «جي بي إس»، أو إغلاقها فوراً[31]. ببساطة، كان يستحيل على الـ «إف بي آي» تتبع 3 آلاف سيارة من دون اللجوء إلى الوسائل الإلكترونيّة المؤتمتة؛ فالوكالة ليست لديها قوة عاملة كافية لإنجاز تلك المهمة. حاضراً، مع انتشار الخلوي، أصبح من الممكن ملاحقة كل شخص، كل الوقت.

مثال آخر تقدمة الماسـحات الضوئيّة للوحات ترخيص السيارات، وهي أجهزة تزداد شيوعاً باطراد. إذ يحتفظ عدد من الشركات بقاعدة بيانات عن لوحات رخص السيارات التي تخلف أصحابها عن دفع قروض مركباتهم. هناك كاميرات مثبتة فوق سيّارات الملاحقة وشاحنات الجرّ، تعمل بصورة متواصلة على مسح لوحات رخص المركبات السـائرة على الطرق، وإرسـال البيانات إلى الشركات بحثاً عن المتخلّفين. ومع وجود أموال كثيرة كامنة في تجارة إعادة تملك المركبات[32]، ينخرط في العملية أشـخاص كثر - ويرسـلون جميعهم معلومات تصب في قواعد بيانات مركزية عند

الشركات. زعمت إحدى شركات الملاحقة، اسمها «فيجيلانت سوليوشنز أوف ليفرمور» (Vigilant Solutions of Livermore) ومقرّها كاليفورنيا، أنها تمتلك 2.5 بليون سجل[33]، وتجمع 70 مليون صورة مسح رقمي للوحات السيارات شهريّاً، مع معلومات عن التاريخ والوقت والموقع وفق نظام الـ «جي بي إس».

إضافة إلى تجارة إعادة تملك السيّارات[34]، تبيع شركات القارئات الضوئيّة معلوماتها إلى محامي الطلاق والمحققين الخاصين، وغيرهم. تبث تلك الشركات بياناتها أحياناً مباشرة إلى أقسام الشرطة التي تعمل على ربطها مع معلومات المسح الآتية من مداخل الطرق السريعة، ومراكز دفع رسوم المرور على الطرقات الرابطة بين الولايات، ونقاط عبور الحدود، ومواقف السيّارات في المطارات. وتبحث الشرطة عن مركبات مسروقة، وسائقين صدرت بحقهم مذكرات قضائيّة، ومخالفات غير مدفوعة. يضاف إلى ذلك أن الـ «إف بي آي» دأبت على الاستفادة من قواعد المعلومات عن رخص القيادة[35] للتعرّف إلى الأشخاص؛ وعملت «وزارة الأمن الوطني» على توحيد تلك المعلومات كلها في قاعدة بيانات موحّدة على المستوى الوطني[36]. في المملكة المتّحدة، هناك قاعدة بيانات مماثلة[37] تستند إلى كاميرات الرقابة الثابتة المنشورة في طول البلاد وعرضها. وتدعم تلك البيانات إنفاذ نظام لندن لضريبة ازدحام المرور(*)، والعثور على المركبات المتأخرة عن الاختبارات الإلزامية لصلاحية سيرها على الطرقات[38].

يجدر بك أن تتوقّع حدوث أمر مماثل مع انتشار تقنية التعرّف المؤتمت إلى الوجوه[39]. في البداية، الأرجح أن تستعمل الصور التي تلتقطها الكاميرات الرقميّة الخاصة من قِبل حاصدي المكافآت، الذين يتتبعون أثر المتهربين من الكفالات القضائية. مع ذلك، ستباع تلك الصور في النهاية لاستخدامات أخرى ثم تصل إلى الحكومة. تملك الـ «إف بي آي» للتو قاعدة بيانات تحتوي 52 مليون وجه[40]، مع

(*) يفترض بالمركبات عدم المرور في وسط لندن بين أول النهار وآخره، معظم الأسبوع، وتغرّم المركبات المخالِفَة.

برامـج كفؤة في التعرّف المؤتمت إلى الوجوه. وتسـتخدم شرطـة دبي حالياً نظاماً[41] يسـتند إلى التكامل بين برامج التعرف إلى الوجـوه وبين «نظارة غوغل»[*] (Google Glass) للتعرف أوتوماتيكيّاً على المشـتبه فيهـم. ومع توفر أعداد كافية من كاميرات الرقابـة في المدينة، سـيتمكن ضبّاط الشرطـة من ملاحقة السـيّارات والناس في كل مكان، من دون مغادرة مكاتبهم.

هـذه هـي الرقابة العامـة، المسـتحيلة مـن دون كومبيوترات، وشـبكات، ونُظُم أتمتة. وليس شـعارها «لاحق تلك السيارة»، بل «لاحق كل سيّارة». كان باستطاعة الشرطـة دومـاً تعقّـب من تشـتبه به، لكن بوجود شـبكة مـن الكامـيرات في المدن، وماسحات لوحات السـيارات، وبرامج التعرف إلى الوجوه، تستطيع الشرطة الآن تعقّب الجميع – سواء مشتبه فيهم أم لا.

على نحو مُشـابِه، كانت عملية شـبك أداة اسمها «سجل القلم» على خط الهاتف الأرضي لمشـتبه فيـه، بهـدف تسـجيل الأرقـام التـي يتصل بهـا، مكلِفَة ومسـتهلكة للوقت. أما الآن فتسـتطيع «وكالة الأمن القومي» الحصول على تلك المعلومات من قواعـد البيانات لشركات الهاتف[42]، بل تسـتطيع الحصول على معلومات عن كل شخص في الولايات المتّحدة. وقد فعلت ذلك.

في العام 2008، اسـتحدثت شركة «وييز» (Waze)– التي استولت عليها شركة «غوغـل» عام 2013 – نظامـاً جديداً لتتبع الأمكنة على الهواتف الذكيّة. وتتلخّص فكرته في أن الشركة تستطيع استعمال المعلومات المتأتيّة من رصد تحرّكات السيّارات التـي تسـتخدم نظـام «وييـز»[43] في اسـتخلاص بيانـات مرورية في زمـن حقيقي، وتوجيـه الناس صوب أسرع الطرق وأقلها ازدحامـاً. بالطبع، كلنا نرغب في تجنّب اختناقات المرور، وفي الحقيقة لا يستفيد مستخدمو نظام «وييز» وحدهم بل المجتمع

(*) نظـارة تربـط بكومبيوتـر صغير يقدّم معلومات عما يشـاهده مرتديها، ويتدخّل في المشـاهدة نفسـها أيضاً، بحذف غير المرغوب رؤيته وإضافة العكس.

برمتـه عندما يُبعَد الناس عن الطرق المختنقة مروريّاً فلا يزيدون في تفاقم المشـكلة. لكن، هل نعرف كمية المعلومات التي نفرط بها ونقدّمها لذلك النظام؟

لأول مرة في التاريخ، تمتك الحكومات والشركات القدرة على ممارسة رقابة عامة عـلى شـعوب بأكملها. ويمكنهـا فعل ذلك عبر اسـتخدامنا الإنترنـت، واتصالاتنا الهاتفيـة، وتعاملاتنـا الماليـة، وتحركاتنا... وكل مـا نفعله. حتى الألمـان الشرقيون لم يستطعوا تعقب كل شخص كل الوقت، في حين أصبح ذلك سهلاً الآن.

رقابة خفيّة

إذا كنت تقرأ هذا الكتاب على جهاز «كيندل» (Kindle) للقراءة الإلكترونيّة[44]، فلسـوف تعـرف ذلـك فـوراً شركـة «آمـازون» (Amazon) التي تصنعه. سـتعرف «كينـدل» متى بدأت القـراءة، وكم كانت سرعتك فيها، وما إذا كنت قرأت الكتاب بشـكل متواصل، أم كنت تكتفي بقراءة بضع صفحات منه يوميّاً، وإذا كنت قفزت إلى نهايتـه، ثـم عـدت ثانية لتقرأ أحـد الفصول، وإذا وضعت علامـات على إحدى الصفحـات. وسـوف تعـرف شركة «آمـازون» كل ذلك أيضاً. لا تلتمع أي إشـارة ضوئيّة، ولا يظهر أي مربع حوار يحذّرك بأن «كيندل» يرسل إلى «آمازون» معلومات عن عاداتك في القراءة، بل يحدث الأمر هكذا ببساطة، وبهدوء واستمرارية[45].

نحـن نتسـاهل حيال مسـتوى من الرقابـة الإلكترونيّة على الإنترنـت لا نقبل به في العـالم الفعـلي، لأنه ليس واضحاً ولا معلناً. فأن يطلـب منك موظّف إبراز بطاقة هويّتـك، أو أن تلتقط كاميرا كشـك المرور صورة اللوحة المعدنية لسـيارتك، أو أن يطلـب جهاز الصراف الآلي («إيه تي إم/ ATM ») بطاقتك مع الرقم الخاص بالشريحة الإلكترونيّة لتلك البطاقة، أمر مختلف عن الرقابة. صحيح أن كل تلك الأفعال تنتج سـجلات رقابة[46]- والحالة الأولى قد تتطلّب أن ينسـخ الموظف أو يستولي بطريقة مـا عـلى المعلومات المذكورة في بطاقـة هويتك- لكنها على الأقـل حالات واضحة. نحن نعرف أنها تحصل.

معظم عمليات الرقابة الإلكترونيّة لا تحصل على تلك الشاكلة، فهي سريّة. نقرأ الصحف على الإنترنت دون أن ندرك أن المقالات التي قرأناها مسجلة. ونفتش في المخازن الإلكترونيّة دون أن نعرف أن كلا الأشياء التي نشتريها وتلك التي نشاهدها ونقرر ألا نشتريها قيد المراقبة المستمرة. ونستخدم نُظُم الدفع الإلكترونيّة دون أن نفكر في كيفية احتفاظها بسجلات عن مشترياتنا. ونحمل هواتفنا الخلوية معنا دون أن نفهم أنها باستمرار تتعقب المواقع التي نكون فيها.

«بزفييد» (Buzzfeed) موقع شبكي للترفيه، يجمع كميّات ضخمة من المعلومات عن مستخدميه. تأتي معظم تلك المعلومات من الطُرُق التقليديّة في تعقب الناس على الإنترنت، لكن «بزفييد» يحتوي كثيراً من المسابقات المرحة يطرح بعضها أسئلة شخصيّة جداً. أحد تلك الأسئلة هو: «ما مدى حظوتك الاجتماعيّة»؟[47]، ويطلب تفاصيل عن وضعك المالي، واستقرارك الوظيفي، ونشاطاتك الترفيهيّة، وصحّتك العقلية- النفسية. دخل ما يزيد على مليوني شخص تلك المسابقة[48]، دون أن يتنبّهوا إلى أن «بزفييد» يختزن المعلومات من أسئلته ومسابقاته. وعلى نحو مُشابِه، تجمع مواقع المعلومات الطبيّة كـ «ويب ميد» (WebMD) [49] معلومات عن الصفحات التي يفتش القرّاء عنها والتي يقرؤونها.

كي لا تظن أن المعلومات المتأتية من المواقع الشبكيّة التي تزورها، وبريدك الإلكتروني، ومكالماتك الهاتفيّة، و«غرف المحادثة»، وغيرها من وسائل الاتّصال الإلكتروني تخضع وحدها للمراقبة، فإن الرسائل البريديّة الورقيّة قديمة الطراز تخضع أيضا للمراقبة. بواسطة برنامج اسمه «آيسوليشن كونترول أند تراكينغ» (Isolation Control & Tracking)، تصوّر «خدمة البريد الأميركي» الوجه الخارجي الأمامي والخلفي، *لكل رسالة بريد ورقيّة في الولايات المتّحدة*. يشكّل ذلك قرابة 160 بليون قطعة سنوياً[50]. وتتوافر تلك المعلومات لقوى إنفاذ القانون، وبالتأكيد لوكالات حكوميّة أخرى.

بعيداً عن الإنترنت، هناك عدد كبير من تقنيّات الرقابة التي تغدو أصغر حجماً وأقل وضوحاً للعيان. في بعض المدن، تلتقط كاميرات الفيديو صور وجوهنا مئات المرّات يوميّاً. بعضها بارز للعيان تماماً، لكننا لا نستطيع رؤية الكاميرات من نوع «سي سي تي في/ CCTV» المثبّتة قرب ضوء في السقف، أو صراف آلي (إيه تي أم)، أو كامير «غيغابكسل» فائقة القوة تراقبنا من عمارات سكنية مجاورة. كذلك تصغر أحجام طائرات الـ«درون» باطراد وتضحى أكثر خفاءً عن العيون[51]؛ فقد بلغ بعضها الآن حجم الحشرات، وسرعان ما ستصير بحجم ذرات الغبار.

إذا أضفت برامج التعرّف الإلكترونيّ إلى نُظُم جمع الصور، فسوف تحصل على نظام مؤتمت للرقابة الشاملة كاملة القدرة. تعتبر برامج التعرّف إلى الوجوه الطريقة الأسهل لتحديد الأشخاص في صور الكاميرا[52]، وتزداد هذه التقنية تطوّراً سنة بعد أخرى. في عام 2014، صارت الخوارزميّات الرقميّة في التعرف إلى الوجوه أكثر اقتداراً من البشر[53]. هنالك نظم أخرى للتعرّف إلى الصور قيد التطوير: أجهزة لمسح قزحيّة العين تعمل عن بُعد[54]، ونُظُم التعرف إلى طريقة المشي[55]، وهكذا دواليك.

ثمة تزايد في عمليات الرقابة في الشوارع. إذ يمكن تعقّب الناس باستخدام نظام «التأشير بموجات الراديو» [يعرف باسمه المختصر «رفيد» (RFID) (*)][56] وهو موجود في بطاقات الهويّة والبطاقات الائتمانيّة التي تحملها في محفظتك. تتعقّب مجموعة من المخازن الكبرى الناس بطريقة خفيّة[57]، عبر التقاط ما تبثّه بانتظام هواتفهم النقّالة، سواء بنظام الـ «ماك» في الـ «آي فون» أم الـ «بلوتوث»، وهي تتكوّن أساساً من أرقام تلك الهواتف. يسعى ذلك التعقّب إلى معرفة الأقسام التي يرتادونها، والرفوف التي يتوقفون عندها[58]، والبضائع التي يتفحصونها وما إلى

(*) - يتكوّن من سلسلة من الخطوط القصيرة المرصوصة، وهي ترسل موجة راديو خفيفة، كتلك التي تستقبلها الآلات الحاسبة في المخازن، فتتعرف إلى أسعارها.

ذلك. ويمكن تعقّب عامة الناس أثناء مشاركتهم في مناسبات عامة بواسطة هاتين المقاربتين[59].

في 2014، أخبر مسؤول تنفيذي كبير في شركة «فورد موتور» الجمهور في «معرض الإلكترونيّات الاستهلاكية»: «نعرف كل من ينتهك القانون، ونعرف متى تنتهكونه. لدينا أجهزة «جي بي إس» في سياراتكم، لذا نعرف ما تفعلونه». كان لذلك التصريح وقع الصدمة والدهشة، إذ لم يعرف أحد من قبل أن «فورد» تخضع مالكي سيّاراتها لرقابة مستمرة. سرعان ما سحبت الشركة التصريحات، لكن تلك التعليقات أفسحت المجال لكثير من التقلقل بشأن جمع «فورد» معلومات عن مالكي سياراتها[60]. وبفضل تقرير صدر من «مكتب المحاسبة الحكومية»[61]، بتنا نعرف أن شركات صناعة السيارات وصناعة أدوات الملاحة الأرضيّة تجمع بيانات مواقع كثيرة من مستخدميها.

هناك رادارات بنطاق تردّد «تيراهيرتز»[62] تستطيع اكتشاف أسلحة مخبّأة يحملها الناس، وأشياء وأجسام عبر جدران اسمنتية تزيد سماكتها عن 8 إنشات [20 سنتيمتراً تقريباً]. وهناك كاميرات تستطيع «استراق السمع» على مكالمات هاتفيّة بالتركيز على أشياء قريبة من المتحدث[63]، كأكياس البطاطا المقليّة، وقياس الذبذبات الصادرة عنها. وتستطيع «وكالة الأمن القومي»، ونظريّاً المؤسّسات المشابهة، أن تشغّل هاتفك الخلوي عن بُعد، وأن تصغي إلى ما يحدث حولك[64].

ثمة من يعمل على تطوير نُظُم للتعرّف إلى رائحة الأجساد أيضاً[65]. وهناك شركة على الإنترنت تسعى إلى التعرّف إلى الناس من طريقة طباعتهم على لوحة المفاتيح[66] وأسلوبهم في الكتابة[67]. وتحصد الحكومات والشركات معاً عشرات الملايين من البصمات الصوتيّة[68]، التي تمثّل طريقة أخرى في التعرف إليك مباشرة في الوقت الفعلي.

ذلك هو المستقبل. سوف يعرف الموظفون في المتاجر اسمك، وعنوانك، ومستوى دخلك بمجرد عبورك الباب[69]. وسوف تعرفك لوحات الإعلانات في الطرقات، وتسجّل استجابتك لها[70]. وسوف تعرف رفوف محلات البقالة ما تشتريه عادة[71]، وكيف يمكن إغراؤك بشراء مزيد من البضائع. وسوف تعرف سيارتك ركابها[72]، ومن يقودها، وقوانين المرور التي يتقيّد بها السائق وتلك التي يتجاهلها. حتى الآن، يبدو ذلك وكأنه خيال علمي.

مع تلاشي الرقابة في خلفيّة الأشياء، يصبح من الأسهل تجاهلها. وكلما ازداد تطفل نظام رقابة وفضوله، ازدادت أرجحية أن يكون خفيّاً. يرفض كثيرون منا إجراء «اختبار مخدرات» قبل توظيفهم، لكن العديد من الشركات يجري تحقيقات موسعة تسبر خلفيّات موظفيها المحتملين كافة. على نحو مماثل، نشعر حين نكون موضع رقابة من مئات الشركات على الإنترنت- وهي شركات لم نتعامل معها ولا حتى سمعنا بها- بقدر أقل من التدخلية مقارنة بمئة باحث تسويق يلاحقوننا باستمرار، ويسجلون ملاحظات عنا.

بمعنى ما، نعيش في حقبة فريدة من التاريخ؛ فالعديد من نظم الرقابة ما يزال مرئياً لنا. طُرُق التثبّت من الهوية شائعة، لكنها ما تزال تطلب منا إبراز بطاقة هويتنا. وتنتشر الكاميرات في كل الأمكنة، لكننا ما نزال قادرين على رؤيتها. في المستقبل القريب، ولأن تلك النُظُم ستغدو خفيّة، ربما نذعن دون معرفة منا إلى قدر حتى أكبر من الرقابة.

الرقابة المؤتمتة

يطالنا كم مدهش من الرقابة بصورة أوتوماتيكيّة، حتى لو بذلنا ما في وسعنا للخروج من دائرتها. ويجري ذلك لأننا نتفاعل مع الآخرين، وهم أنفسهم قيد المراقبة.

مع أني لم أضع قط تدويناً على «فيسبوك» ولم أصادق أحداً فيه- إذ أملك صفحة مهنيـة لا حسـاباً شـخصيّاً- فإن «فيسـبوك» يتعقبنـي[73]. في قاعـدة بياناته، يحتفظ بملفات فيها «بروفايل» شخصي لمن لا يستعملون «فيسبوك». يلاحقني كلما دخلت صفحة على «فيسـبوك» فيها زر «أعجبني» («لايك»/ Like). والأرجح أنه يستطيع أن يخمّن بصواب كبير من هم أصدقائي[74]، استناداً إلى التذييلات الملحقة بصوري معهم، وربما لديه أيضاً «بروفايل» شـخصي عني ملحقاً بمعلومات أخرى اشـتراها من سـماسرة المعلومات. ومع وجود أصدقاء لي على «فيسـبوك»، وتلك المواقع التي تتضمّن أزرار «أعجبني»، تتاح له مراقبتي.

أحـاول تجنّب اسـتخدام محـرّك البحث «غوغـل»[75]، لكن ذلـك لا يحول دون قدرتـه على جمع المعلومات عـن المواقع التي أزورها؛ لأن عدداً كبيراً منها يسـتعمل أداة «غوغـل للتحليـلات» (Google Analytics) في تتبّع زوّارهم. مرّة أخرى، تتيح تلك المواقع لـ«غوغل» أن يتتبعني بواسطتها. أستخدم أدوات كثيرة للصدّ في محرّك البحث الذي اسـتعمله بهدف منع «غوغل» مـن ملاحقتي بدقة[76]، لكني أعلم أن «غوغل» يعمل على تقنيّات تستطيع احتواء إجراءاتي الأمنيّة كافة.

لا أسـتخدم بريد «جـي ميل» (G-mail) الإلكتروني، بل أسـتفيد بدلاً من ذلك مـن «مقدّم خدمة الإنترنت» (اختصـاراً: «آي بي إس» IPS) المحلي، وأخزّن بريدي الإلكـتروني عـلى كومبيوتـري. مع ذلـك، يملك «غوغـل» ثلث رسـائلي[77]؛ لأن كثيرين ممن أتراسل معهم يستخدمون «جي ميل». ولا يقتصر الأمر على العناوين في موقع «جي ميل.كوم»؛ لأن «غوغل» يسـتضيف مجموعة كبيرة من المؤسّسـات التي تقـدّم خدمـات البريد الإلكتروني، على الرغم من أن تلك المؤسّسـات تحتفظ باسـم نطـاق علوي «دومين نيـم» (Domain Name) خاص بها، فـلا يظهر مصطلح «جي ميل.كـوم» في نهايـة عناوينها. ثمـة أمثلة أخرى كثيرة. تملك شركـة «آبل» (Apple) قاعـدة بيانات عن كلمات المرور على موجات الـ«واي- فاي» (Wi- Fi)، من بينها الـ«واي- فاي» في منزلي؛ تجمعها من الناس كلما أجروا عملية صنع ملفات احتياطيّة

«باك آب» (Back Up) لهواتفهم. وتملك شركات كثيرة معلومات اتّصاليّة عني؛ لأن أصدقائي وزملائي يحتفظون بملفات احتياطيّة عن دفاتر عناوينهم، في مخازن رقميّة ضخمة تسمّى «سحابة معلومات»، أو «كلاود» (Cloud). إذا نشرت أختي ملفاً يحتوي تركيبتها الجينيّة، يصبح نصف تركيبي الجيني معروفاً ومشاعاً عاماً أيضاً.

أحياناً، هناك معلومات نتقصّد مشاركتها مع نفر قليل، لكنها تغدو معلومات متاحة للرقابة عالميّاً. إذ تلتقط إحداهن صورة مع صديق لها في حفلة وتضعها على «فيسبوك»، كي تراها صديقاتها. لكن تلك الصورة تصبح متاحة للعموم ما لم تتقصّد عكس ذلك. وبالطبع، يبقى العثور على تلك الصور أمراً صعباً، إلى أن يتعرّف نظام مؤتمت إلى الوجوه، ويضع تذييلاً خاصاً عليها، ثم يعمل محرّك للبحث على فهرستها. حينها يسهل الوصول إلى تلك الصورة بواسطة محرّك بحث للصور.

أظهَر باستمرار على كاميرات مخصّصة لرقابة آخرين. ففي مدن كلندن وشيكاغو ومكسيكو سيتي وبيجينغ، ثبّتت قوات الشرطة كاميرات رقابة في الأمكنة كافة[78]. وفي مدن أخرى كنيويورك، تعود ملكية كاميرات مماثلة إلى القطاع الخاص. وقد ظهر لنا الفارق بين الأمرين في حادثين إرهابيّين. في لندن، جرى التعرّف إلى مفجّري مترو الأنفاق بواسطة كاميرات الحكومة، أما في ماراثون «بوسطن»، فقد تولّت المهمة عينها كاميرات ملحقة بشركات خاصة.

من شبه المؤكد أن تلك معلومات رقميّة[79]، وغالباً ما تخزّن في الكاميرا على دارة فلمية مغلقة تمحو المعلومات القديمة مع تسجيلها معلومات جديدة. لكن يتزايد الميل إلى وضع فيديو الرقابة ذاك على شبكة الإنترنت، ما يؤدي إلى تخزينه إلى ما لا نهاية - فيغدو قسم كبير منه متاحاً للعموم بواسطة محرّكات البحث.

ما لم نتخذ خطوات لمنع ذلك، سوف تتدنى إلى حد أبعد إمكانيّة تجنّبنا الظهور على كاميرات الآخرين مع زيادة انتشار كاميرات تسجيل الحياة. فحين يقوم عدد كاف من الناس بتصوير ما يشاهدونه بانتظام، سوف تظهر في عدد كافٍ من لقطات

فيديوهاتهـم بحيث لا يعـود مهماً ما إذا كنت تحمل كاميرا وتصور حياتك اليوميّة أم لا. إنه نوع من مناعة القطيع، لكن بطريقة معاكسة.

الرقابة الشاملة

ابتكر الفيلسـوف جيرمي بِنثام تصميمه المعروف باسـم «الرقابة الشاملة» («بان أوبتيكـون»/ Panopticon[*]) [80] في أواخـر القـرن الثامـن عـشر كطريقة أرخص لبناء السـجون. وتتمثّل فكرته في تشـييد سـجن يكون فيه كل نزيل تحت الرقابة كل الوقت، من دون أن يدري. ولا يملك النزيل خياراً سوى افتراض أنّه مراقَب دائماً، ولذلك يذعن ويتكيف مع الوضع. استُخدِمَتْ تلك الفكرة مجازاً لجمع المعلومات الشخصيّة عن الجموع[81]، سواء أكانوا على الإنترنت أم خارجها[82].

على الإنترنت، الرقابة شاملة. كلنا قيد المراقبة[83] كل الوقت، وتلك المعلومات تخزّن إلى الأبد. ذلك ما يبدو عليه حال الرقابة في عصر المعلوماتيّة، وهي أكثر فعاليّة من أشد أحلام بِنثام جموحاً.

(*) يتكوّن المصطلح من مقطعي "بان" (pan) بمعنى «شامل»، و«أوبتكون» (opticon) بمعنى «إبصار»، والمعنى هو سجن يمكن رؤية أو مراقبة كل من فيه على مدار الساعة.

3

تحليل بياناتنا

في العـام 2012، نشرت صحيفة نيويورك تايمس مقالاً يبيّن أن الشركات تحلّل معلوماتنا، خدمة لغايات إعلانية. وكشـف المقال أن شركـة «تارغِت» (Target)(*) تسـتند إلى تحليـل ميول الشراء لدى زبائنهـا لمعرفة إن كُنّ حواملَ أم لا، وتسـتخدم تلك المعلومة بأن ترسل لهن إعلانات وكوبونات عن سلع مخصّصة للمواليد. شمل المقال قصة تفصيليّة عن رجل من مدينة «مينابوليس» الأميركيّة تقدّم بشكوى بصدد قيام «تارغت» بإرسـال كوبونات تتعلق بسـلع المواليد إلى ابنته المراهقة، ثم اكتشف لاحقاً أنّ «تارغِت» كانت على حق[1]!

تسـمّى ممارسـة جمع البيانـات وتخزينهـا بأنواعها كافـة[2] «البيانـات الضخمة» (Big Data)، ويسـمى علم هندسـة اسـتخراج معلومـات مفيدة منهـا «التنقيب في البيانات» (Data Minning). وتنقّب شركات كـ«تارغِت» في البيانات لتركيز حملاتها الإعلانيـة. الرئيس بـاراك أوباما اعتمد على أسـلوب التنقيب الكثيـف في البيانات أثناء حملتيه الرئاسـيتين في 2008 و2012، للهدف نفسـه[3]. وتنقّب الشركات في المعلومـات التـي تحصل عليها من سـيّاراتكم، كي تصنع سـيارات أفضـل؛ وتنقّب البلديات في البيانات التي تحصل عليها من المجسّات المنشورة في الطرقات كي تفهم

(*) تعتبر شركة "تارغِت" ثاني أكبر شركات أميركا للبيع بالتجزئة، بعد شركة "وال مارت" (Walmart) الشهيرة.

ظـروف قيـادة المركبات. ويجـري التنقيب في المعلومـات عن تراكيبنـا الجينيّة خدمة لأنـواع البحـوث الطبيّة كافـة. وتنقّب شركات كـ «فيسـبوك» و«تويـتر» في بياناتنا لغايـات إعلانيـة، كما سـمحت للعلماء بالتنقيـب في تلك البيانـات خدمة للبحوث الاجتماعيّة[4].

تمثّل تلك الأمور كلها الاسـتخدامات الجانبيّة للبيانات. ويقصد من ذلك القول إنها لا تمثّل السـبّب الأصلي لجمع المعلومات. الحال أن الوعد الأساسي لـ «البيانات الضخمة» هو: «خزّن كل ما تسـتطيع الوصول إليه، وسـيكون مسـتطاعاً ذات يوم التوصّل إلى شيء ما مفيد منها».

تملـك «البيانات الضخمة» قيمة مشـتقّة جزئيّاً من الاسـتنتاجات التي يمكن أن تسـتخلص منها. بعـض تلك الاسـتنتاجات واضح تمامـاً. إذا امتلكـتَ معلومات مكانيّة عن تحرّكات شـخص ما خلال سـنة بأكملها، بإمكانك أن تسـتنتج المطاعم المفضّلـة لديـه. إذا حـزتَ قائمـةً بالأشـخاص الذيـن يتحـدث إليهـم ويراسـلهم إلكترونيّـاً، فبإمكانـك أن تسـتخلص من هـم أصدقـاؤه. وإذا كانت لديـك قائمة بمواقـع الإنترنت التي يـتردّد عليها- أو ربما قائمة الكتب التي اشـتراها- فيمكنك أن تستنتج اهتماماته.

بعض الاسـتنتاجات أكثر فطنة. قائمة مشـتريات البقالة لشـخص ما قد توحي بإثنيّتهـا، أو عمرهـا وجنوسـتها، وربـما دينهـا، أو تاريخهـا الطبي وعادتهـا في تناول المشروبـات الروحيّة. ويتحرّى المُسـوّقون باسـتمرار عن أنماط يمكـن أن تنبئ بأن شـخصاً مـا على وشـك الإنفاق ببـذخ، كإقامـة حفـل زواج، والذهـاب في عطلة، وشراء منـزل، وقـدوم مولود، ومـا إلى ذلك. في بلدان عدّة، تسـتخدم الشرطة تلك البيانات كأدلة إثبات، إما سراً أو أمام المحاكم. ويمكن لحسـاب على «فيسـبوك» أن يـشي بمعلومات عن الأصل العرقي لمسـتخدمه وشـخصيته[5]، خياراته الجنسـيّة، أيديولوجيتـه السياسـيّة، وضعيـة علاقاتـه الشـخصيّة، واسـتخدامه مـواد مكيّفة؛

ويجـري ذلـك كلـه اسـتناداً إلى مجـرد التعـرّف إلى أنـماط اسـتعماله لـزر «لايك» في «فيسـبوك». يستطيع «فيسـبوك» أن يعرف خطوبتك قبل إعلانها[6]، أو كونك مثليّ الجنس قبل أن تقرّر إشهار ذلك علانية[7]- بل إن التدوينات عليه ربما تكشف تلك الأمور للآخرين من دون إذنك ولا حتى معرفتك[8]. ووفقاً للبلد الذي تقطنه، من المحتمل أن تشكل تلك الأمور إحراجاً كبيراً، أو ربما تتسبّب في مقتلك[9].

هناك عدد كبير من الأخطاء في تلك الاستدلالات، وكثيرون منا اختبروا وصول إعلانـات بواسـطة الإنترنت إليهـم، ولم تكن تعنيهـم فعليّاً إلا بأقل مـن القليل. في المقابـل، عندما تصيـب تلك الإعلانات هدفها[10] فإنها تثير خضّة مرعبة، وغالباً ما تكـون ممجوجة. هناك فارق كبير بين الحالين. أنت ترى أحياناً إعلانات عن تحاميل طبيّة لعلاج البواسـير، أو إعلانات على التلفزيون عن خدمات تساعدك في التعرّف إلى فتـاة بغرض الصداقة، وحينها، تكون على علـم بأنها إعلانات عموميّة وموجهة إلى الجمهـور بمجملـه. ثمـة فارق كبير بـين تلك الحـال، وبين أن تصلنـا إعلانات تكون موجّهة إلينا تحديداً[11]، ومستندة إلى تدويناتنا على الإنترنت أو مواقع زرناها على الشـبكة، فتبـدو كأنها نوع من الاجتياح. إذ يتولّد عـن ذلك توتّر مثير للاهتمام: المعلومـات التي رغبنا في مشـاركتها مع الآخرين تقود إلى اسـتنتاجات لا نرغب في التشارك بها أبداً. يرحب عديدون بأن يقدموا لشركة «تارغِت» معلومات عن أنماط مشـترياتهم للحصـول على تخفيضات وإشـعارات بخصوص منتجـات جديدة ربما يرغبـون في شرائها؛ لكن معظمنا ربما لا يرغـب في أن يخبر «تارغِت» بحدوث حال حمل. وكذلك فإننا لا نستسيغ عمليات السرقة والسطو على المعلومات التي تضرب بصورة محتّمة قواعد المعلومات المتصلة بـ «البيانات الضخمة».

حـين نفكـر بـأنّ الكومبيوتـرات تسـتخدم كل معلوماتنا في صنع اسـتدلالات واستنتاجات عنا، نصل إلى طريقة إنسانيّة تماماً في التفكير بصدد تلك الآلات. نحن نفكر في ما يمكن أن نسـتنتجه من المعلومات، ثم نُسـقِط ذلك على الكومبيوترات. ليسـت تلـك بطريقـة صائبـة للتفكـير بشـأن الحواسـيب. ثمـة فـوارق في القـوى

والمحدّدات ونقاط الضعف، بين البشر والكومبيوترات. إذ لا يستطيع الكومبيوتر ممارسة التفكير المجرّد مثلما يفعل معظم البشر، لكن الآلات تستطيع التعامل مع كميّات كبيرة من المعلومات، وبطريقة تتزايد سرعتها باستمرار. (من المستطاع التفكير بأن ذلك يعني أن الكومبيوتر متفوّق في التعامل مع «البيانات الوصفيّة»، أكثر من التعامل مع تفاصيل المكالمات والحوارات). وتتزايد قوّة الكومبيوترات باطّراد، إذ ما زالت قوّتها تتضاعف كل 18 شهراً، فيما يظل حجم دماغ الجنس الإنساني ثابتاً. وحاضراً، تتفوّق الحواسيب على البشر في التعامل مع المعلومات الكميّة، بل إن قوّتها تتحسّن على نحو مطّرِد.

في الوضع الراهن، يمثّل التنقيب في المعلومات تقنية «ساخنة»[12]، بمعنى أنها موضع اهتمام فائق، إضافة لكونها محاطة بكثير من الادّعاءات والهالات والانتهازيّة. ليس من الواضح كليّاً أنواع البحوث الممكنة في ذلك الحقل، ولا القوى الكامنة فعليّاً فيه. في المقابل، من البيّن أن تقنية التنقيب في البيانات تتزايد قوّتها، وتعطي المراقبين قدرة متعاظمة على التوصّل إلى استنتاجات مذهلة من المجموعات المتراكمة من «البيانات الضخمة».

الرقابة في أزمنة مضت

ثمة شيء جديد يمكنك فعله بتطبيق تقنية التنقيب في البيانات على الرقابة العامة، يتمثّل في الرجوع إلى الماضي[13]. إذ تمحورت الرقابة التقليديّة على الحاضر والمستقبل: «راقب ذلك الشخص، وتعرّف إلى خطوته التالية». ولكن، عندما تحوز قاعدة معلومات فيها معلومات متراكمة زمنيّاً عن كل شخص، حينها تستطيع فعل شيء جديد: «دقّق في تلك «المعلومات المكانيّة» عن ذلك الشخص، وتعرّف إلى الأمكنة التي يوجد فيها»؛ أو «استمع إلى مكالماته أثناء الأسبوع الماضي».

في المـاضي، كانـت بعض تلك الأشـياء ممكنة أيضاً. وتاريخيّـاً، دأبت الحكومات على جمع كل أنواع المعلومات. ففي الحقبة المكارثيّة(*) على سـبيل المثال، اسـتخدمت الحكومة سـجلات الأحزاب السياسـيّة، والاشتراكات في المجلات، وشهادات من الأصدقـاء والعائلة والجيران والزملاء؛ بهـدف جمع المعلومات عن الناس. والفارق بـين ذلـك المـاضي وما يحدث حـاضراً يتمثّـل في أن القدرة عـلى الرقابة باتت تشـبه صنـع آلة الرجـوع إلى الماضي: إذ صارت البيانات أكثر دقّـة واكتمالاً، وتدنّت تكلفة الحصول عليها، وتطوّرت التكنولوجيا بما يعطي القدرة على الإتيان بتحليل تاريخي متطوّر. مثلاً، في السنوات القليلة الماضية، أقرّت بنوك «كريدي سويس» و«ستاندرد شارتر» و«بي آن بي باريبا»، بأنّها اخترقت قوانين حظر نقل الأموال إلى مجموعات قيد المعاقبة. وغيّرت المؤسّسـات تلك البيانات للتملّص من ترصد الجداول الخوارزميّة ورقابتها لـ «فلاتر أوفاك»، وهي اختصار لـ «مكتب رصد الأصول الماليّة الأجنبية» التابـع لـ «الخزانة العامة» الأميركيّة. واسـتلزم التعرّف إلى ذلـك النوع من التملّص الجرمـي[14] إجـراء تحليل تاريخي مكثّف لأزمنة المعامـلات الماليّة والاتّصالات بين الموظّفين.

وعلى نحو مشـابه، من المسـتطاع اسـتخدام أدوات تحليليّة مبتكـرة، للتنقيب في معلومـات قديمـة. لنفكر في البيانـات عن التركيبـة الجينيّة للأفراد. حـاضراً، ليس هنـاك الكثير مما يمكن اسـتخلاصه من تحليل التركيبـة الجينيّة للفرد، لكن بعد عشر سـنوات- مـن يعرف كيف تكـون الأمور حينها؟ لقد رأينا شـيئاً مشـابهاً يحصل في اختبـارات المنشـطات في سـباقات «تور دي فرانـس» للدراجات الهوائيّـة. وعندما جرى تحليل عيّنات دم أخذت قبل سـنوات من درّاجين[15]، بواسـطة أساليب أكثر جدّة؛ تفجّرت فضيحة انتشار المنشطات في تلك المنافسة.

(*) إشـارة إلى فترة في مطالع الخمسـينيات من القرن العشرين، اسـتطاع فيها السـيناتور الجمهوري جو مكارثي تحريض الحكومة الأميركية على ممارسة رقابة واسعة تحت شعار محاربة الشيوعية.

تختزن «وكالة الأمن القومي» سيولاً من المعلومات المتراكمة من أزمان ماضية، وهو أمر سأتحدّث عنه بتفصيل أكبر في الفصل الخامس. نعرف أنّه في العام 2008، كان لدى الوكالة قاعدة معلومات تسمّى «إكس كي سكور» (XKEYSCORE)[16]، تحتفظ روتينياً بتسجيلات صوتيّة للمكالمات لمدة ثلاثة أيام، لكنها تخزّن الـ «ميتاداتا» عنها لمدة شهر كامل. وفي قاعدة بيانات أخرى لـ «وكالة الأمن القومي» تحمل اسم «مارينا» (MARINA)[17] تجمع معلومات عن عمليات تصفّح الجمهور للـ «ويب» لمدة سنة. وفي قاعدة بيانات أخرى اسمها «ميستيك» (MYSTIC)[18]، احتفظت الوكالة بتسجيلات المكالمات الهاتفية كافة، التي تمر من تحت مياه جزيرة «برمودا» وهي محطة رئيسة للكوابل البحريّة للاتّصالات بواسطة الهواتف الأرضيّة، التي تصل بين أميركا ومعظم الدول الغربيّة. وتحتفظ الوكالة بـ «ميتاداتا» الهواتف لخمس سنوات[19].

تنطبق حدود تلك المدد الزمنية للتخزين على المعلومات كافة. وفي حال تلمّس أحد عملاء الوكالة شيئاً ما في قواعد المعلومات، تحتفظ الوكالة بذلك النوع من البيانات لمدة أطول. إذا كانت المعلومات عنك متأتيّة من بحث استقصائي في تلك القواعد للبيانات، يجري الاحتفاظ بها إلى الأبد. إذا استخدمت التشفير، يجري الاحتفاظ بمعلوماتك إلى الأبد[20].

تتعلّق مدة تخزين المعلومات لدى «وكالة الأمن القومي» بالقدرات التقنيّة أكثر من احترامها الخصوصيّة. نعرف أن الوكالة احتاجت لزيادة قدراتها على تخزين كل المعلومات التي جمعتها عن مواقع الهواتف الخلوية[21]. ومع التدني المستمر في تكلفة تخزين البيانات، يمكن التفكير بأن مزيداً منها سيُحتَفَظ به لمدد أطول. عند تلك النقطة[22]، تظهر الفكرة من «مركز يوتاه للمعلومات» الذي أنشأته «وكالة الأمن القومي».

تحتفـظ وكالـة الــ «إف بي آي» بالمعلومـات أيضـاً[23]. وفي غـمار تحقيـق قانوني جـرى في 2013، حصلت الـ «إف بي آي» على نسـخة عن البيانـات الموجودة كافة في موقع يسـّمى «فريدوم هوستنغ» (Freedom Hosting)، بما في ذلك رسائل البريد الإلكتروني المخزّنة عليـه. كانت معظم البيانات غير متعلّقة بالتحقيق مباشرة، لكن الـ«إف بي آي» احتفظت بنسخة عن الموقع برمّته؛ ومنذها، باتت تدخل عليه تكراراً أثناء تحقيقات لا تتعلق به. وتحتفظ ولاية نيويورك بمعلومات عن القارئات الضوئيّة للوحات المركبات، لخمس سنوات على الأقل وربما إلى ما لا نهاية[24].

من المستطاع مبدئيّاً الاحتفاظ بالمعلومات كافة كسجلات التواريخ في «فيسبوك»، والتغريـدات، وصـور لوحات المركبات، إلى ما لا نهايـة، أو إلى أن يتقرّر حذفها من قِبَـل الشركة أو الوكالـة الحكومة المعنية. في 2010، كانـت شركات الخلوي تحتفظ بالرسـائل النصيّة لما يتراوح بين 90 يوماً و18 شـهراً. وتفوّقت عليهم جميعاً شركة «إيـه تي أنـد تي» (AT&T)[25]، بـأن توصّلـت إلى الاحتفاظ بتلك الرسـائل لسـبع سنوات.

وضع خرائط العلاقات

تفتـح المعلومـات المسـتقاة من الرقابـة العامة الباب أمـام إمكانيّة رسـم خرائط للعلاقات الشـخصيّة بـين الأفراد. في 2013، عندما عرف النـاس للمرّة الأولى أن «وكالـة الأمـن القومي» دأبت على جمـع «بيانات وصفيّة» عـن مكالمات الأميركيّين كلهـم، ثار ضجيج كبير حول ما سُـمّي «البحوث النطّاطة» ومـا تعنيه فعليّاً. إذ إنّها تمثّـل نوعـاً جديداً مـن البحوث كانت ممكنـة نظريّاً قبل عـصر الكومبيوتر، لكنها لم تغـدُ عمليّةً بصورة فعليّة إلا بعد الرقابـة الرقميّة العامة. تخيّل مثلاً أن «وكالة الأمن القومي» وجّهت اهتمامها صوب فتاة ما تدعى آليس. سوف تجمع الوكالة معلومات عن تلك الفتاة، ثم معلومات عن كل الأشخاص الذين اتّصلت بهم، ثم معلومات عن الأشـخاص الذين اتّصلوا بأولئك الأشـخاص، ثم معلومات عن الأشـخاص

الذيـن اتّصل الأخيرون بهم. بذا، تكون الوكالة على بُعد ثلاث «قفزات» من آليس، وهو الحدّ الأقصى الذي تعمل الوكالة في نطاقه.

يتمثّـل القصد من «البحوث النطّاطة» في رسـم خريطة عن العلاقات والتحري عـن وجـود تآمر مـا. وكي تغدو تلـك المعلومات مجديـة[26]، يجب استبعاد غالبية سـاحقة من أشـخاص أبريـاء في تلك الشـبكة المُتَصَيّـدة، وأرقام الهواتـف المألوف اسـتخدامها من قِبَل أولئـك الأبرياء[27]: شركات خدمة البريـد الصوتي، ومطاعم الـ «بيتزا»، وشركات سيارات الأجرة، وهكذا دواليك.

تشـير وثائق «وكالة الأمن القومي»[28] إلى أنها لاحقت 117675 «هدفاً ناشطاً للرقابة» في يوم واحد في 2013. وإذا اسـتخدمنا التقديرات الأشـد تحفّظاً عن عدد الأشـخاص الذين يتحدث إليهم المرء ومدى تشـابكهم مع آخرين، سوف يتجاوز العدد الكلي للأشـخاص الموضوعين قيد الرقابة في ذلك اليوم بسـهولة ما يربو عن 20 مليون شخص[29]. يعطي ذلك مثلاً كلاسيكيّاً عن مسألة «الحلقات الست» في العلاقات بين الناس، بمعنى أن هناك عموماً سـت دوائر (أو سـت «قفزات»)، وفق تعابـير «البحوث النطّاطة») تفصل بين كل شـخص وآخـر في الولايات المتّحدة. في العـام 2014، طلب الرئيس بـاراك أوباما[30] من «وكالة الأمن القومي» أن تقتصر «البحـوث النطّاطة» عـلى «قفزتين» في تحليـل «البيانات الوصفيّـة» لأرقام الهواتف الموضوعـة تحت رقابة برنامج ما للوكالة، لكـن الرئيس لم يضع قيوداً على عدد تلك «القفزات» في الأنواع الأخرى من المعلومات التي تجمعها الوكالة.

تشكّل «البيانات الوصفيّة» المستقاة من مصادر متنوّعة أداة قويّة في رسم خرائط العلاقات الشـخصيّة. إذ تستخدم غالبيتنا الإنترنت في التواصل الاجتماعي بواسطة الـ «سوشال ميديا»، وتظهر علاقاتنا الشخصيّة فيها. كذلك فإنّه بالضبط ما تتشارك فيه معاً «وكالة الأمن القومي» وشركة «فيسـبوك»[31]، وهو السـبب في أن الأخيرة

تقترح عليك ببرود أسـماء أشـخاص ربما تكون تعرفت إليهـم، لكنك لم تضعهم في قائمة الأصدقاء في حسابك على «فيسبوك».

يتمثّل أحد أكثر مناحي برامج «فيسبوك»[32] الإعلانية نجاحاً في عدم اقتصارها على إبراز الإعلانات الترويجيّة على شاشـات كل مَـن ضغط على زر «أعجبني» عند مشاهدة سلعة أو صفحة، بل أيضاً إلى أصدقائهم ثم أصدقاء أصدقائهم أيضاً.

التحري عنا بأفعالنا

بعد أن تتجمع المعلومات عن كل شخص، يصبح ممكناً العثور على كل فرد بتتبع سلوكيّاته. ربما رغبت في معرفة كل من يتردّد على مقصف مخصص للمثليّين جنسيّاً، أو يطالـع مواضيع معيّنة، أو يمتلك أفكاراً سياسـيّة محدّدة. تتـولى الشركات معرفة تلك الأمور بصورة منتظمة بواسـطة استعمال معلومات الرقابة الرقميّة العامة، كي تعثـر على مسـتهلكين محتملين لهـم تفضيلات معيّنـة، أو إيجاد أشـخاص ترغب في توظيفهم بواسطة البحث عمن نشر أشياء عن موضوعات بعينها.

من المستطاع التفتيش عن أشياء غير الأسماء والمُعرّفات الشخصيّة الأخرى كرقم الهويّة والهاتف وغيرهما. مثلاً، يفتش «غوغل» كل رسـائلك في «جي ميل»[33]، ثم يسـتخدم الكلمات المفتاحيّة التي عثر عليها، كي يتوسّـع في فهم شخصيتك، وذلك لغايـات تتعلق بالإعلانـات. تفعل «وكالة الأمـن القومي» أمراً مُشـابِهاً[34]، لكنها تسـمّيه «بحوث الـ «حَوْلَ»». وبصورة أساسيّة، يعمل ذلك النوع من البحوث عبر التفتيش في محتوى الاتّصالات لشخص ما، بحثاً عن كلمات أو أسماء معيّنة- أو ربما عبارة بعينها. فإذاً، إضافة إلى التفتيش في البيانات المتعلقة بآليس والأشخاص الذين تشـملهم «قفزتان» أو ثلاث «قفزات» حولها، تسـتطيع الوكالة أن تفتش معلومات الأشـخاص كافـة- بمعنى التفتيش في قواعـد بيانات الاتّصالات كافـة- بحثاً عن اسـمها. وإذا لم تكن الوكالة على معرفة باسـم آليس، لكنها تعرف مشروعاً أو مكاناً أو اسماً حركيّاً يستخدمه أحدهم في الإشارة إلى آليس؛ تستطيع إجراء بحوث انطلاقاً

مـن تلك المعلومات. ومثلاً، تسـتهدف «وكالـة الأمن القومي» الأشـخاص الذين يبحثـون عن أدوات رقميّـة تتعلق بالخصوصيّة على الإنترنت أو بإخفاء الشـخصيّة عليها[35].

لا نعـرف التفاصيـل، لكـن «وكالة الأمـن القومي» تعمد إلى ربط سلاسـل من «البحـوث النطّاطـة»[36]، انطلاقاً مـن أي علاقة تقع تحت يدهـا؛ ولا يقتصر الأمر على الاتّصالات الهاتفيّة. إذ يحتمل أن يشـمل ذلك الربط وجودك في المكان عينه مع شـخص تحت الرقابة[37]، أو وجود أشخاص مشتركين بينك وبينه في الاتّصالات، وما إلى ذلك. بات ممكناً إجراء تلك الأنواع من البحوث بفضل القدرة على الوصول إلى بيانات الناس كلها.

من المسـتطاع اسـتخدام الرقابة العامة للعثور على أشـخاص معيّنين. إذا علمت أن شـخصاً مـا كان في مطعـم معـين في ليلة بعينهـا، وقصد محطة مـترو ذات ظهيرة بعد ثلاثة أيام، واقترب من محطة كهرومائيّة في الصباح التالي؛ تسـتطيع إجراء تحقيق في قواعـد البيانـات عن مواقع الهواتف للناس كافة، فيظهر فوراً الأشـخاص الذين تنطبق عليهم المواصفات السابقة.

مـن المسـتطاع أيضاً التفتيش عن السـلوك الخـارج عن المألوف. في مـا يلي أربعة أمثلة عن الطرق التي تستعملها «وكالة الأمن القومي» في تحليل معلومات الخلوي.

(1) تسـتعمل الوكالة «المعلومات المكانيّة» للخلـوي[38]؛ كي تتبع الأفراد الذين تتقاطـع مواقـع أمكنتهـم. لنفـترض أن الوكالـة مهتمـة بآليـس. إذا تبين أن شـخصاً اسـمه بوب كان في المطعم الذي قصدته آليس ذات مساء، وكذلك في المقهى الذي تناولت فيه القهوة صباحاً بعد أسبوع، وفي نفس المطار الذي توجّهت إليه آليس بعد شهر؛ سوف يشير النظام المعلوماتي للوكالة إلى بوب بوصفه مشاركاً محتملاً مع آليس، حتى لو لم يتواصل الشخصان إلكترونيّاً.

(2) تتعقّب الوكالة مواقع أجهزة الخلوي التي يحملها جواسيس أميركا في الخارج[39]، ثم تحدّد إذا كان ثمة خلوي آخر يتتبّع الهاتف المحمول لأحد جواسيس أميركا. وأساساً، تتعقّب الوكالة إذا كان ثمة من يلاحق أولئك الجواسيس.

(3) تملك الوكالة برنامجاً لتصيّد «البيانات الوصفيّة» عن الهواتف[40]، يستطيع ملاحظة الخلويات التي استُعمِلت لفترة وجيزة ثم أقفلت ولم يُعَاود أحد تشغيلها لاحقاً أبداً. وتستخدم الوكالة المعلومات عن أنماط استخدام الخلويات كي تربط بينها. وتوظّف تلك التقنية لمعرفة الهواتف «المحروقة»، بمعنى أنها استُخدِمَت من قِبَل أشخاص يسعون لتجنّب الرقابة.

(4) تجمع الوكالة معلومات عمّن أطفأوا هواتفهم، إضافة إلى المدة التي تبقى فيها مطفأة[41]. ثم تجمع بيانات عن الأمكنة التي يعاود فيها أولئك الأشخاص تشغيل هواتفهم فيها. وكذلك تجمع معلومات عن أشخاص آخرين أغلقوا هواتفهم في أمكنة قريبة من المجموعة الأولى. بقول أوضح، تسعى الوكالة إلى رصد الاجتماعات السريّة.

سبق أن ناقشتُ الطريقة التي استخدمت فيها الحكومة الأوكرانيّة «المعلومات المكانيّة» عن الخلويات، بهدف التعرّف إلى كل من شارك في تظاهرات معارضة لها، وكذلك الأمر بالنسبة لاستعمال شرطة ولاية «ميشغن» لـ «البيانات المكانيّة» عن الخلويات للتعرّف إلى من كانوا قرب مكان لتجمع نقابي احتجاجي مزمع. وتستعمل الـ «إف بي آي» تلك البيانات لملاحقة خلويات يستعملها أشخاص تحت الرقابة، لكن لا تربطها بهم علاقات أخرى[42].

تفعل الشركات أشياء مشابهة أيضاً. ثمة تقنية تسمّى «التطويق الجغرافي»، يستعملها المسوّقون للتعرف إلى الأشخاص عندما يكونون قرب مراكز تجاريّة

معيّنة، كي تُرْسـل لهم موادَّ إعلانية. تقـدّم إحدى شركات «التطويق الجغرافي»[43]، اسمها «بلايس كاست» (Place cast)، إعلانات تجاريّة مستندة إلى المواقع الجغرافيّة، وترسلها إلى عشرة ملايين خلوي في الولايات المتّحدة والمملكة المتّحدة، كي تصلهم عندما يكونون قرب سلاسل المخازن الكبرى كـ«ستارباكس» (Starbacks) و«كاي مارت» (K Mart) و«ساب واي» (Subway). تفعل شركة «مايكروسوفت» الأمر نفسه مع الأشـخاص الذين يمرون على مسـافة عشرة كيلومترات من مخازنها[44]؛ وهـي تتعامـل مع شركة تعمـل في «التطويـق الجغرافي» اسـمها «نواينث ديسـيميل» (NinthDecimal). وتسـتعمل شركة «سـينس نتوركس» البيانـات المكانيّة للخلوي كي تصنع ملفات «بروفايل» عن الأفراد[45].

تنسيق المجموعات المتنوّعة من البيانات

تعـدُّ «فيجيلنـت سوليوشـنز» (Vigilant Solutions) مـن الـشركات التي تجمع بيانـات عن لوحات المركبـات من الكامـيرات[46]. وتملك الشركـة خططاً لتدعيم نظامهـا المعلوماتي بجـداول خوارزميّة أخرى تفيد في التعرّف إلى أرقام السـيّارات، ونُظُم التعرّف إلى الوجوه، ومعلومات من قواعد أخرى للبيانات. والنتيجة المتوقعة هـي منصة رقابة أشـد صرامة ودقـة من مجرد قاعـدة للبيانات فيها صـور للوحات المركبات، بغض عن النظر عن الاتساع الذي تصل إليه تلك المنصة.

غالبـاً مـا يضـع الإعـلام وقصصـه الإخباريّـة الرقابـة العامة ضمـن إطار جمع المعلومـات والبيانـات؛ ولكن تفوته حكاية الربط والتنسـيق بين المعلومات، بمعنى ربط الهويّات[47] الموجودة في مجموعات متباينة من قواعد البيانات؛ بهدف التوصل إلى استنتاجات واستدلالات من البيانات المجمّعة. لا يتعلق الأمر بمجرد القول إن طائرات «درون» أرخص ثمناً سـتصبح أمراً شائعاً تماماً، فيما كاميراتها ستكون أشد قـوة. تتمثّل المسـألة في أن الـ «درون» مع برنامج رقمي للتعرّف إلى الوجوه سـيتيح للنظـام التعـرّف إلى الناس بطريقة مؤتمتـة، إضافة إلى وجود قواعـد بيانات ضخمة

للصـور المذيّلـة بتعريفات عمن فيها- وهي مسـتقاة من رُخَـص القيادة وصفحات «فيسـبوك» والصحف اليوميّة والكتب السـنويّة للمدارس الثانويّة- وكلها مصادر ترفد ذلك البرنامج بصور مرجعيّة للأفراد. وكذلك تتعلّق المسـألة بالربط والتنسيق بـين مخرجات ذلـك البرنامج للتعرّف، مـع قواعد بيانات متنوّعـة أخرى؛ ويُضاف إليهـا القـدرة على تخزيـن كل تلك المعلومات إلى مـا لا نهاية. تتأتى الرقابة الشـاملة مـن جمع سـيول المعلومات والبيانـات الآتية من مصادر مختلفـة، وربطها معاً في كلٍّ متكامل.

عندما أكون في لندن، أسـتخدم بطاقة من شركة «أويستر»[48] [تتميّز بأن بياناتها لا تصل إلى الإنترنت] لدفع بدل النقل في المواصلات العامة. بذلت قصارى جهدي وعنائـي كـي أبقي على دفع بدل النقل نقـداً، ودون التعريف إلى الهوية. وعلى الرغم مـن ذلك، إذا جرت مقارنة اسـتعمال تلك البطاقة مع قوائـم زوار لندن وتواريخها، سـواء أكانت تلك القائمة من صنع خطوط الطـيران، شركات البطاقات الائتمانيّة، شركات الخلـوي، أم «مقدّمـي خدمات الإنترنت»؛ فأنا أراهن على أنني الشـخص الوحيـد الذي سـوف تتقاطـع عنده تلك المعلومـات بتكامل تام. لـذا، فإن تحرّكاتي «الخفية الاسم» في مترو أنفاق لندن، لا تحقّق ذلك الهدف أبداً.

كشـف سـنودن مشروعاً مثيراً للاهتمام تنهض به مؤسّسـة «سيسك» (CSEC)، وهـي اختصـار لاسـم «مؤسّسـة أمـن الاتّصـالات في كنـدا» (Communications Security Establishment Canada)، وهـي نظـيرة «وكالة الأمـن القومي» في ذلك البلـد. ويبرهـن المشروع أهمية الربط والتنسـيق بين مسـارات مختلفـة من معلومات الرقابة للعثور على أشخاص يتقصّدون التملّص منها[49].

ثمـة باحـث في «سيسـك» تحمـل وظيفتـه لقبـاً جذّابـاً هـو «مطـوّر مهـارات الجاسوسـيّة»، انطلق مما يسـاوي معلومات لمدة أسـبوعين جُمِعَت مـن الإنترنت، ما يعني أساساً أنه عمل على قوائم تعرّف إلى أرقام الهويّة للذين دخلوا إلى مواقع مختلفة

على الإنترنت. وكان لديه أيضاً قاعدة بيانات عن المواقع الجغرافية لأرقام التعريف عن المستخدمين للشبكات اللاسلكيّة للإنترنت. وبمقارنة مجموعتي المعلومات، استطاع ذلك الباحث التوصّل إلى ربط أرقام هويّات من دخلوا إلى الإنترنت بواسطة شبكات لاسلكيّة، مع مواقعها الجغرافيّة. كانت الفكرة من البحث هي العثور على أشخاص. إذا كان لديك رقم هوية استخدام الإنترنت لشخص قيد الرقابة، تستطيع أن تطلق صافرة إنذار عند دخوله شبكة لا سلكيّة للإنترنت في مطار أو فندق، وبالتالي معرفة موعد سفره. وكذلك تستطيع أن تتعرّف إلى شخص معين بمعرفتك المواقع الجغرافية التي عبرها مع التواريخ والأوقات. مثلاً، لنفترض أنك تبحث عن شخص اتّصل بك من دون أن يكشف هويّته، من ثلاثة مواقع لهواتف عموميّة. أنت تعرف أزمنة تلك المكالمات ومواقع التليفونات التي أجريت منها. إذا كان في جيب ذلك الشخص هاتف ذكي، فإن الأخير يتّصل بصورة أوتوماتيكيّة مستمرة مع الشبكات اللاسلكيّة، ما يمكّنك من الربط بين تلك الاتّصالات الأوتوماتيكيّة وبين الأوقات والتواريخ التي لديك، وكذلك مواقع تلك الشبكات. والأرجح أنك ستصل بالنتيجة إلى التعرّف إلى شخص بعينه.

توصّل بحاثة في «جامعة كارنيجي ميلون» إلى فعل شيء مشابه. إذ وضعوا كاميرا رقابة في مكان عام، والتقطوا صوراً لأشخاص يمرون بها، وتعرّفوا إليهم بفضل برامج التعرّف إلى الوجوه مع قاعدة بيانات «فيسبوك» عن الصور المذيّلة بتعريفات، ثم قارنوا الأسماء مع قواعد أخرى للبيانات. وبالنتيجة توصلوا إلى إبراز معلومات شخصيّة عن الأفراد الذين يمرون بالكاميرا، في لحظة مرورهم بها فعليّاً[50]. ومن المستطاع توفير تلك التقنية لكل شخص، بواسطة استعمال كاميرا ذكيّة أو ارتداء نظّارة «غوغل».

أحياناً، يسهل الربط بين الهويّات الموجودة في قواعد بيانات مختلفة؛ فاسمك مربوط مع هاتفك الخلوي، وكذلك الحال بالنسبة لبطاقتك الائتمانيّة. أحياناً، تكون الأمور أكثر صعوبة. إذ ربما لا يكون اسمك مربوطاً فعليّاً ببريدك الإلكتروني،

إلا في حال أشار من تتراسل معهم إليك بالاسم. هناك شركات كـ «إنيشييت سيستمز» (Initiate Systems)، تبيع برامج رقميّة تربط بين المعلومات الموجودة في قواعد بيانات مختلفة[51]؛ وهي تبيع تلك البرامج إلى شركات وحكومات. كذلك تعمل الشركات على الربط بين سلوكك على الإنترنت وبين أفعالك الحقيقيّة خارج الإنترنت. ومثلاً، يتشارك موقع «فيسبوك» مع سماسرة المعلومات كشركتي «إبسلون» (Epsilon) و«آكسيوم» (Acxiom)، للمقارنة بين بروفايلك الشخصي في «فيسبوك» وبين مشترياتك في المخازن الكبرى[52].

عندما تتوصل إلى الربط بين مجموعات مختلفة من المعلومات، يغدو باستطاعتك فعل أشياء عدّة بها. تخيل أنك تريد صنع صورة عن صحة شخص ما، من دون أن تعرف ملفه الطبي. تستطيع بيانات البطاقات الائتمانيّة وبطاقات الشراء من المخازن الكبرى، أن تعطي معلومات عما يفضّله من مأكولات وما يتناوله من مشروبات كحوليّة، وكذلك المطاعم التي يقصدها، وإذا كانت لديه عضويّة في مركز للرياضة، وماهيّة الأشياء التي يشتريها من الصيدليّات خارج الوصفات الطبيّة.

ويكشف هاتفه الخلوي عدد المرات التي يقصد فيها المركز الرياضي، وتقدّم أدوات رقابة الحركة معلومات عن مستوى نشاطه البدني هناك. وتكشف البيانات عن المواقع الشبكية التي يستعملها عن نوع المعلومات الطبيّة التي يهتم بالتفتيش عنها. بواسطة تلك الطُرُق، تتمكن شركة كـ «إكزاكت داتا» (Exact Data) من بيع قوائم عن الأشخاص الذين ينخرطون في المواعدة بواسطة الإنترنت[53]، والمقامرين، وأولئك الذين يعانون أمراضاً كالقلق النفسي والتبوّل اللاإرادي أو اضطراب القدرة على الانتصاب.

اختراق خفائنا

عندما تتنصّت منظّمة قويّة على قسم كبير من بنيتنا الإلكترونيّة التحتيّة، مع قدرتها على الربط بين مسارات مختلفة من الرقابة، فإنّها تستطيع في الغالب أن تتعرّف إلى الأشخاص الذين يسعون إلى الخفاء. في ما يلي 4 قصص تبرهن ذلك الأمر.

(1) جرى التعرّف إلى الـ «هاكرز» العسكريّين الصينيّين[54]، الذين شاركوا في مجموعة واسعة من الهجمات ضد الحكومة والشركات الأميركيّة؛ لأنهم دخلوا إلى موقع «فيسبوك» مستخدمين البنية الإلكترونيّة التحتيّة نفسها التي استعملوها في تنفيذ هجماتهم.

(2) أخضع هكتور مونزيغر[55]، أحد قادة حركة الـ «هاكرز» تحمل اسم «لولزسيك» (LulzSec)، للتحقيق لأنه اخترق عدداً من الشبكات التجاريّة، بعد أن تمكّنت الـ«إف بي آي» من التعرف إليه واعتقاله في 2011. وعلى رغم أنه أركن إلى عادات حسنة في أمن الكومبيوتر كما استخدم هويّة مغفلة في الحصول على وصلة لدخول الإنترنت، فإنه انزلق ذات مرّة. وإذ لم يستطع تجنب الإشارة إلى نفسه أثناء إحدى المحادثات، استطاع محقّق في الـ«إف بي آي» أن يتتبعه وصولاً إلى الحصول على فيديو من موقع «يوتيوب» (YouTube)، عن سيارته، ثم عثر على صفحته في موقع «فيسبوك».

(3) في سياق مشابه، اتّخذت باولا بردويل[56] التي أقامت علاقات جنسية مع مدير الـ «سي آي إيه» الجنرال ديفيد بيترايوس، احتياطات واسعة بهدف إخفاء هويتها. ولم تدخل أبداً على بريدها الإلكتروني الذي لا يحمل هويّتها من منزلها. وبدلاً من ذلك، استعملت شبكات في فنادق وأماكن عامة للتراسل مع بيترايوس. وقارنت الـ «سي آي إيه» معلومات التسجيل من فنادق مختلفة، وسرعان ما ظهر اسم مشترك (باولا بردويل) بينها.

(4) هناك «هاكر» سمّى نفسه «ورمر» وكان ناشطاً ضمن مجموعة الـ «هاكرز» المعروفة باسم «أنونيموس» (Anonymous) [57]، كما كان مطلوباً بسبب اختراقه مواقع أمنية أميركيّة. واستخدم حساباً غفل الهويّة على «تويتر»، لكنه وضع صورة لصدر امرأة التقطها بهاتف «آي فون». وتضمّن ملف الصورة معلومات الـ «جي بي إس» عنها، ما أتاح تحديد أنها التُقِطَت في منزل في أستراليا. وهناك موقع آخر، أشار إليه «ورمر»، لكنه كان يتضمن اسم هيغينيو أوشاوا أيضاً. وتراقب الشرطة صفحة أوشاوا على «فيسبوك» التي تضمّنت معلومة تفيد بأن لديه صديقة أستراليّة. وتطابقت صور تلك الصديقة مع الصورة الأولى التي انطلق منها التحقيق. وبذا، استطاعت الشرطة أن تعتقل أوشاوا الذي يحمل اسماً حركيّاً هو «ورمر».

يكاد إخفاء الهويّة أن يكون مستحيلاً على الإنترنت حيال مراقب كليّ القدرة. إذا نسيت لمرّة تفعيل حماياتك، إذا ضغطت على رابط إلكتروني لا يجدر بك التعامل معه، إذا طبعت شيئاً ما بالخطأ؛ تربط اسمك بشكل دائم مع من قدّم لك خدمة إخفاء الهويـة على الإنترنت. إنّ المستوى العملاني للاستمرار في الاحتفاظ بالخصوصيّة وإخفاء الهويّة على الإنترنت، في مواجهة تحقيق موجّه ومصمّم على الوصول إليك، يفوق مصادر حتى العملاء الحكوميّين المدربين جيّداً. وحتى فريق اغتيال إسرائيلي مدرب على مستوى متقدّم، انكشف بسرعة في دبي، استناداً إلى تذييلات كاميرات الرقابة في المدينة[58].

ينطبق الأمر عينه على مجموعات كبيرة من البيانات المُغْفَلَة الهويّة. لربما راودنا الاعتقاد الساذج بأن عددنا كبير إلى حدّ أنّه من المستطاع الاختباء في ذلك البحر من البيانات؛ أو أن معظم معلوماتنا خفيّة الهويّة. كل ذلك ليس صحيحاً. إذ إنّ معظم

تقنيّات إخفاء الهويّة فاشلة[59]، ومن الممكن إعادة وضع الهويّة على البيانات انطلاقاً من معلومات فائقة الضآلة.

في العام 2006، أصدرت شركة «إيه أو إل» (AOL) بيانات عن عمليات التفتيش على الشبكة التي أجراها 657 ألف مستخدم، وبلغ عددها قرابة 20 مليون عملية. قصدت الشركة أن تكون البيانات مفيدة للبحّاثة، لذا سعت إلى حماية هوية الأشخاص باستبدالها بأرقام. لنقل إنها أعطت الكاتب بروس شناير رقماً هو 608429. وتفاجأت الشركة عندما تمكّن البحّاثة من التوصّل إلى الأسماء[60]، بواسطة ربط المُكوّنات المختلفة في ملف عمليات التفتيش التي أجراها الأفراد على الإنترنت.

في 2008، نشرت شركة «نتفلكس» (Netflix) عشرة ملايين تقييم للأفلام عبّرت عن آراء نصف مليون مستخدم، لم تكشف عن هويّاتهم. جاءت الخطوة ضمن تحدٍّ أطلقته الشركة للجمهور العام بأن يأتي بنظام لتقييم الأفلام أفضل مما كانت الشركة تستعمله في ذلك الوقت. واستطاع بحّاثة أن يتعرّفوا إلى الهويّات المغفلة للمستخدمين[61]، بمقارنة التقييمات وتذييلات الوقت مع ما يقابلها في موقع «إنترنت موفي داتا بيز» (Internet Movie Database)، الذي يعدُّ أضخم قاعدة بيانات عن أفلام السينما يتفاعل معها جمهور الإنترنت.

ربما بدت تلك الأمثلة كأنها تعبّر عن حالات خاصة، لكن فرص ملاحظة عمليات ربط البيانات تتكرّر بأكثر مما تظن[62]. إذا استطاع شخص ما النفاذ إلى قاعدة بيانات لأرقام الهواتف لا تحتوي على أسماء، فإنّه يستطيع التوصل إلى معرفة أسماء أصحابها بربطها بقاعدة بيانات عن مكالمات تسوّق البضائع وطلبيّاتها. وعلى نحو مشابه، يمكن استعمال قاعدة بيانات مراجعة الكتب في موقع «آمازون» كمفتاح للتعرف ولو بصورة جزئيّة، إلى الهويّات المغفلة في قاعدة بيانات عن المشتريات بواسطة بطاقات الائتمان.

استناداً إلى معلومات عامة لا تأتي على ذكر الهويّة، في الإحصاء السكاني في أميركا للعـام 1990، اسـتطاعت المختصّة في علـوم الكومبيوتر لاتانيا سـويني أن تتعرّف إلى هويّـة 87 ٪ مـن سـكان الولايات المتّحـدة، ما يسـاوي 216 مليونـاً من أصل 248 مليون شـخص، بواسـطة الربط بين أرقام المناطق البلديّة المخصصة للأفراد، مـع قواعد بيانات عن نوعهم الجنسي وتواريـخ ميلادهم. في نصف تلك الحالات، كان يكفي الانطلاق من اسـم المدينة، البلـدة، أو البلديّة، للوصول إلى معرفة الهويّة الفردية[63]. واستطاع بحاثة آخرون التوصل إلى نتائج مماثلة[64]، استناداً إلى بيانات الإحصاء السكاني للعام 2000.

ومـع قاعدة بياناته الهائلة عن جمهور الإنترنت، يسـتطيع محرّك البحث «غوغل» التعرّف إلى الهويات الفردية في قاعدة بيانات عن المشـتريات بواسـطة الإنترنت، أو الأسـماء في قاعدة بيانات طبيّة عن الجمهور العام. ويستطيع التجّار الذين يحتفظون بمعلومات تفصيليّة عن الزبائن ومشـترياتهم، استخدام تلك المعلومات في التعرّف إلى هويّـات الأفـراد في قواعـد البيانـات الكـبرى لأي محـرّك للبحث، ولـو بصورة جزئيّـة. وكذلك يسـتطيع سمسـار للمعلومات يحـوز قواعد بيانـات لمجموعة من الـشركات، التوصّـل إلى معرفة الهويّـات الفردية في معظم سـجلات تلك القواعد، بواسطة مقارنتها بعضها بعضاً.

توصّل باحثون إلى معرفة هويّة الأفراد اسـتناداً إلى معلومات عن أحماض وراثيّة لا تتضمـن هويّـات أصحابهـا[65]، بمقارنة تلـك المعلومات مع بيانـات من مواقع التحري عـن الأصول العائليّة والعرقية وغيرها. وحتى بيانات البحوث النفسـيّة-الجنسـيّة التي أجراها آلفرد كينـزي[66] في ثلاثينيات القرن الماضي وأربعينياته لم تعد مأمونـة. وعلى الرغم من الجهود المضنية التي بذلها كينزي في إخفاء هوية المشـاركين في تلك البحوث، اسـتطاعت الباحثة راكيل هيل التعرّف إلى هويّات 97 ٪ منهم في العام 2013.

ربـما لا تبدو تلـك الأمور متوافقة مـع البداهة العامة والحس السـليم[67]، لكن لا يسـتلزم الأمر سـوى قليل من البيانات (أقل مما نعتقـد بكثير) للتوصل إلى تحديد الهويّـة الفرديّـة لمعظم الناس. وعلى الرغم مـن أننا نبدو عاديّين تمامـاً، فإننا فريدون جداً. ومثلاً، تبيّن أنه إذا جرى حذف الأفلام المئة الأكثر مشـاهدة، يظهر أن عادات مشـاهدة الأفلام هي فرديّة تماماً. ينطبق أمر مماثل على عادات قراءة الكتب بواسـطة الإنترنـت، عـادات المكالمـات الهاتفيّـة، عـادات التفتيش عـلى المعلومات بواسـطة الشـبكة، والـشراء بواسـطة الـ «ويب». من المسـتطاع التعـرّف إلى فرادتنا بواسـطة علاقاتنـا[68]. ومـن الواضـح أنـه يمكن التعـرّف إليك تحديـداً بواسـطة «البيانات المكانيّة» عنك. ومع معلومات تنسـكب على مدار السـاعة مـن هاتفك الخلوي عن أمكنتك، من المستطاع التوصّل إلى اسمك من دون عناء كبير. الأرجح أنه لا توجد حاجة لكل تلك المعلومات، إذ يمكن تحديد 95 ٪ من الأميركيّين بالاسـم اسـتناداً إلى 4 نقاط تقاطع للبيانات عن الوقت والتاريخ ومواقع الأمكنة[69].

تبدو الإجراءات المضادة المباشرة ضد تلك الأمور غير فعّالة على نحو مؤسـف. إذ جعلت بعض الشركات مجموعات من بياناتها مغفلة الهويّة بإزالة بعض المعلومات منها، وتغيير تذييلات الوقت، أو تتعمد إدخال أخطاء مقصودة في أرقام الهويّة التي وضعتها بديلاً للأسماء الفعليّة. وسرعان ما تبيّن أن تلك المناورات لم يكن من شأنها إلا جعل عملية الكشف عن الأسماء الحقيقيّة أكثر صعوبة بقليل[70].

واسـتناداً إلى تلك الأسـباب جميعها، تكون القوانين التـي تركّز على «المعلومات المُعرَّفَة بالشـخصيّة» غير مجدية[71]. وفي العادة، تشمل تلك المعلومات الاسم، رقم حسـاب متمتّـع بالفـرادة وما إلى ذلـك؛ إضافة إلى قوانـين مرتبطة بذلـك النوع من المعلومات. في المقابل، تتعلّق «المعلومات المُعرَّفَة بالشخصيّة» بكميّة البيانات أيضاً، فكلـما زادت المعلومـات التي يعرفها شـخص عنك، حتى لو غابـت عنها هويّتك، زادت فرص أن يتعرّف إليك بسهولة أكبر.

في معظـم الأحوال، تتمحـور حماياتنا حول سياسـات الخصوصيّة في الشركات التـي نتعامل معهـا، لكنها لا تتعلّق بالتقنية والرياضيات. ولا يجدي كثيراً اسـتبدال الهويـة برقـم فريد خاص بها. إذ لا يحول ذلك دون الاسـتمرار في جمع عمليات جمع المعلومات ومقارنتها واسـتخدامها، وفي نهايـة المطاف يرجح أن يبدر عنا تصرّف ما يؤدي إلى الربط بين اسمنا وملف معلوماتنا «المغفَل الهويّة».

في عـصر الرقابـة الكليّـة القدرة المتّسـمة بأن الكل يجمـع المعلومـات عنا طوال الوقـت، تضحي الخصوصيّة هشّـة تماماً. ويفـترض بنا إما اللجـوء إلى تقنيّات أكثر متانة في الحفاظ على الخصوصيّة، أو التخلي عن فكرة الحماية بأكملها.

4

تجارة الرقابة

تشكل قدرة الهواتف الحديثة على الإتيان بأشياء مضافة عدّة إحدى الأشياء الأشد إثارة للدهشة. لا يرتدي الناس ساعات لأن هواتفهم فيها ساعة. لا يحمل الناس كاميرات لأنها صارت مكوّناً معيارياً في معظم الهواتف الذكيّة.

من المستطاع أيضاً استعمال ومضات «فلاش» كاميرا الخلوي، لصنع نظام إشارة ضوئي. يعمل التطبيق الرقمي «برايتست فلاش لايت فري» (Brightest Flash Light Free) [1]، على «فلاش» الهواتف التي تعمل بنظام الـ «آندرويد»، وهو تطبيق صنعته شركة «غولدن شورز» (GoldenShores). يعمل التطبيق بشكل جيد، ويتضمن مجموعة من الميّزات الجذّابة. وذهبت بعض المراجعات عن ذلك التطبيق إلى التوصية بوضعه في متناول الأطفال عندما يتسلون بأحد ألعاب الاختباء والمراوغة. هناك ميزة في التطبيق لم تتناولها المراجعات الكثيرة عنه، هي أنّه يجمع باستمرار بيانات عن مكان مستخدمه[2]، مع إمكانية مفترضة ببيعها لمُعلنين.

فعليّاً، حال التطبيق «برايتست فلاش لايت فري» هي أكثر تعقيداً من ذلك. إذ تعتمد سياسة الخصوصيّة فيه، بغض النظر عن قلّة من يقرؤها، على مخادعة المستخدمين بفعاليّة. وتنص على أن الشركة تستطيع استخدام المعلومات التي يجمعها التطبيق، لكنها تتجنب ذكر إمكانيّة بيعها إلى جهات أخرى. وعلى الرغم من أن المستخدمين يجب عليهم أن يضغطوا على زر «أوافق» بالنسبة لاتفاقيّة السماح

باستخدام التطبيق، تبدأ عملية جمع المعلومات عن موقع المستخدم وإرسالها إلى الشركة، حتى قبل الضغط على ذلك الزر.

أثار الأمر دهشة معظم الـ50 مليون مستخدم للتطبيق، عندما كشف خبراء عنه في العام 2012 [3]. وتدخّلت «اللجنة الفيدرالية للتجارة» في المسألة[4]، مجبرة الشركة على كشف ممارساتها المخادِعة وحذف البيانات التي جمعتها. لكن اللجنة لم تفرض غرامة على الشركة؛ لأن التطبيق كان مجانيّاً.

تخيّل لو أن الحكومة الأميركيّة سنّت قانوناً يلزم مواطنيها جميعهم بحمل أجهزة تتبّع. في تلك الحال، سيعدُّ القانون فوراً مخالفاً للدستور. ومع ذلك، فإننا ندأب على حمل هواتفنا معنا في الأمكنة كلها. إذا أجبرتنا قوات الشرطة على إبلاغها كلما عقدنا صداقة جديدة، ستثور الأمة بأكملها. ومع ذلك، فإننا نبلغ ذلك إلى «فيسبوك». إذا طلب جواسيس البلاد نسخاً عن مكالماتنا الهاتفيّة ومراسلاتنا البريديّة كلها، سيرفض الشعب الانصياع. لكننا نقدّم نسخاً عن رسائلنا الإلكترونيّة كلها لمن يقدّم لنا خدمة الـ«إيميل»، وشركات الخلوي، ومنصات التواصل الاجتماعي، ومقدّمي خدمات الإنترنت.

تحدث نسبة ضخمة من الرقابة على يد الشركات، وهي تحدث ذلك بذريعة أننا نوافق عليها. لا أقصد بذلك أننا نتطلع ثم نتّخذ قراراً بالموافقة، بديلاً عن ذلك تأتي موافقتنا إما لأننا نعطي قيمة للخدمة التي نحصل عليها، أو لأن صفقة متكاملة قُدّمَت إلينا تتضمن الرقابة[5]، لكننا لا نملك خياراً حقيقيّاً حيالها. تلك هي الصفقة التي عرضتها في المقدّمة.

يتناول هذا الفصل مسألة رقابة الإنترنت علينا، لكن لنتذكّر أيضاً أن الأشياء كلها متصلة بالإنترنت، أو أنها ستصبح قريباً كذلك. إن رقابة الإنترنت هي تعبير مختصر عن الرقابة في عالم يترابط بعضه بعضاً بواسطة الإنترنت.

يشكّل الإعلان التجاري الهدف الرئيس لكل ما تستهدفه الشركات من رقابة الإنترنت. ثمة سوق جانبي صغير في ذلك المضمار، وكذلك خدمات الزبائن، لكن تلك النشاطات كلها تبدو أمراً هامشياً بالمقارنة مع هدف بيع الأشياء للجمهور.

بصورة تقليديّة، تستند رقابة الإنترنت على شيء ما يسمّى «الكعكات المحلاة» أو «كوكيز» (Cookies). يبدو الاسم مسالماً وحميداً، لكن الوصف التقني له بأنّه «المُعرّف الدائم» هو أشد دقّة بما لا يقاس. في الأصل، لم يقصد من الـ«كوكيز» أن تكون أدوات للرقابة، بل صُمّمت كي تجعل الإبحار بواسطة الإنترنت أكثر سهولة. وليس من طبيعة مواقع الانترنت أن تتذكّرك عند كل زيارة وكل طرقة على الـ«ماوس». قدّمت الـ«كوكيز» حلاً لتلك المعضلة. تحتوي كل «كوكي» على رقم فريد يتيح للموقع التعرّف إليك. وبذا، كلما تجوّلت في موقع للشراء على الإنترنت، كأنك تدأب على القول: «أنا المستخدم صاحب الرقم 608431». ويتيح ذلك للموقع العثور على حسابك عليه، والاحتفاظ ببطاقة للمشتريات ملتصقة بك، وتذكّرك عندما تزور الموقع ثانية وهكذا دواليك.

سرعان ما أدركت شركات الإنترنت أن بوسعها الوصول بالـ«كوكيز» الخاصة بها إلى صفحات على مواقع شبكيّة أخرى، ما أدى إلى ولادة ظاهرة «كوكيز من طرف ثالث». وشرعت شركات كـ«دوبل كليك» (Click Double) [6]– اشتراها محرّك البحث «غوغل» عام 2007 – في تتبّع مستخدمي الإنترنت أثناء تنقلهم بين المواقع المختلفة. وعند تلك النقطة، صار بإمكان الإعلانات ملاحقتك بواسطة شبكة الـ «ويب» كلها. فتّش بواسطة الإنترنت عن سيّارة معيّنة، أو بلدة لقضاء الإجازة فيها، أو وضع صحيّ معيّن؛ ولسوف تستمر بعدها في تلقي إعلانات من شركة تلك السيّارة أو البلدة أو شركة الدواء المتعلّق بالوضع الصحي الذي أجريت بحثاً عنه.

وتطـوّر الأمر لاحقـاً إلى تركيب رقابي خانق بامتداده وقوّتـه وربحيته. ثمة كثير مـن الرقابـة التي تلاحقـك أينما ذهبت أثنـاء وجودك على الإنترنـت، وهي تأتي من الـشركات وسـماسرة البيانات: هنـاك عشرة منها عـلى ذلك الموقـع، وعشرون على موقع آخر وهكذا دواليك. يلاحقك «فيسبوك» في المواقع كلها بواسطة زر «لايك» (سـواء دخلت إلى حسـابك على «فيسـبوك» أم لا). ويتابعك «غوغل» في كل موقع يحتوي على زر «غوغل+» (Google+) أو يسـتعمل أداة التحليل الإحصائي «غوغل آناليتكس» (Google Analytics)، لقياس حركة الزوار عليه.

تملـك معظـم الـشركات التـي تلاحقـك عـلى الإنترنت[7] أسـماء ربما لم تسـمع بهـا: «روبيكـون بروجكـت» (Rubicon Project)، «آد سـونار» (Ad Sonar)، «كوانكاست» (Quancast)، «بالس 260» (Pulse 260)، «آندرتون» (Undertone)، «ترافـك ماركـت بلايـس» (Traffic Market Place). إذا أردت أن تـرى مـن يلاحقـك[8]، أضف إلى محرّك البحث الذي تسـتعمله إحدى الأدوات الرقميّة التي تتيـح لـك رصد الـ «كوكيـز» التي تلاحقك. أضمن لك أنك سـتفزع. إذ اكتشـف أحد المراسـلين الصحافيّين أن 105 شركات مختلفة لاحقته أثناء استعماله الإنترنت لمدة 36 سـاعة[9]. في العام 2010، زرعت شركة لا تثير الريبة، «دكشـينري.كوم» (Dictionary.com)، ما يزيد على 200 «كوكيز» لكل من زار موقعها[10].

لا يختلف الأمر على هاتفك الذكي. وهناك، تلاحقك التطبيقات أيضاً. وتترصد التطبيقـات أمكنتـك، وأحيانـاً تنقـل إليهـا «دفـتر العناويـن» في هاتفـك الخلوي، ومفكرتك، والمواقع التي وضعت إشـارة عليها، وتاريخ عمليات البحث. في العام 2013، توافـق مغني الـ «راب» جاي- زي وشركة «سامسـونغ» (Samsung) على أن يقدّما لمن ينزلون تطبيقاً رقمياً معيّناً، فرصة الاستماع إلى ألبومات جاي- زي قبل إطلاقها في السـوق. ويشـترط ذلك التطبيق عند وضعه عـلى الخلوي[11]، الحصول على كل الحسـابات الموجودة على الهاتف، وتتبع مواقع أمكنته، ومعرفة الأشـخاص الذيـن يتصل بهم مسـتعمله. وذهـب تطبيق رقمي عـن لعبة «العصافـير الغاضبة»

(«آنغـري بـيردز»/ Angry Birds)، إلى حـد طلـب مواقع الأمكنة، حتـى عندما لا يمارس المستخدم تلك اللعبة[12].

وتفـرض الشركات التي تقـدّم خدمة الاتّصـال بالإنترنت بالموجـات العريضة النطاق «برودباند» (Broad Band) كـ«كومكاست» (Comcast)، رقابة مستمرة على مستخدميها[13]. وتنشغل الشركة حاضراً في معرفة إذا ما كنت تحصل على نسخ غير مرخصـة مـن الأغاني وأشرطة الفيديو، لكن الشركات الأخرى ليسـت بعيدة كثيراً عن تلك الممارسة. إذ تعمل «مايكروسـوفت» و«فريزون» (Verizon) وغيرهما[14]، على صنع جهاز لاتّصال التلفزيون بالإنترنت، يستطيع أن يرصد ما يجري في الغرفة كي تتخذ من تلك المعلومات قاعدة للإعلانات التجاريّة.

لا يشـبه الأمـر وجود «الأخ الكبـير»(*) الأورويلي[15]، بل هـو أقرب إلى وجود بضع مئات من الإخوة الوشاة الصغار.

وحـاضراً، صـارت رقابة الإنترنـت أكثر صرامة مـن الـ «كوكيـز». واقعيّاً، ثمة سـباق تسـلح صغير في ذلـك المضمار. محـرّك البحث الذي تسـتعمله- نعـم، بما في ذلـك «غوغل كروم» (Google Chrome)- يملك ضوابط قويّة بإمكانه وقف عمل الـ«كوكيـز»، ويعمد عدد من الناس إلى تفعيل تلـك الضوابط. يعدُّ برنامج «دونت تراك مي» (DoNotTrackMe) من أشـهر الإضافات الإلكترونيّة التي يمكن إلحاقها بمحـرّكات البحـث. ورد صُنّـاع رقابـة الإنترنـت على ذلـك البرنامـج وأمثاله بأن صنعوا «فلاش كوكيز»- هي تتألّف أساساً من ملفات تشبه الـ«كوكيز» ويُحتَفَظُ بها ضمن برنامج «آدوبي فلاش بلاير» (Adobe Flash Player) الذي يتعامل مع ملفات الـ«بي دي أف» والمواد المرئيّة- المسـموعة. وبـذا، تبقى الـ«فلاش كوكيز» حتى بعد أن تتخلـص محـرّكات البحث من الـ«كوكيـز» التي ألصِقَت بهـا. وللتصدي لذلك

(*) "الأخ الكبير" هو الديكتاتور الحاكم في دولة شـموليّة تراقب الجميع، في رواية الكاتب الإنكليزي جورج أورويل 1984.

النـوع من الـ«كوكيز»، تسـتطيع اللجوء إلى برنامج «فلاش بلـوك» (FlashBlock). ولكـن، هنـاك طـرق أخـرى كي تسـتفرد بـك الرقابـة[16]، بواسـطة برامـج تحمل أسـماء شـيفريّة كـ «إيفركوكيز» (evercookies)، و«كانفاس فنغـر برنتنغ» (canvas fingerprinting)، و«كوكيز سـينكينغ» (cookies synching). ولا يقتصر الأمر على المسوّقين. ففي العام 2014، توصّل باحثون إلى أن موقع «البيت الأبيض» استخدم الـ«كوكيز» متعدّياً على سياسـته بالذات بشـأن الخصوصيّة. سـأقدّم بعض النصائح بخصوص صدّ رقابة الـ«ويب» في الفصل 15.

كجـزء من طبيعتها، تخفي الـ«كوكيز» هويّات من تتعامل معهم، لكن الشركات تربـط بينهـا وبين معلومات أخرى تفيد في التعريف عن هويّاتنا بشـكل حاسـم. إذ أنـت تعرّف عن نفسـك طواعيّة لعدد من خدمات الإنترنـت. وغالباً ما تفعل ذلك باسـتخدام اسـم مسـتخدم خاص بك، لكن سرعان مـا يغدو مسـتطاعاً الربط بين اسمك فعليّاً وأسماء المستخدم التي تستعملها. حاول «غوغل» فرض ذلك بواسطة ما سـمّاه «سياسـة الاسـم الحقيقي»[17]، بمعنى الطلب من مسـتخدمي «غوغل +» التسـجيل فيه بأسـمائهم القانونيّة، لكنه ألغى تلك السياسة في 2014. إلى حدّ بعيد، يطلب «فيسـبوك» الاسم الحقيقي[18]. وعندما تسـتخدم بطاقتك الائتمانيّة في شراء شيء مـا، يجري ربـط هويّتك الحقيقيّـة بـ «كوكيز» تعطيها لك الشركـة التي تتعامل معهـا. وفي كل مرّة تسـتخدم هاتفك الخلـوي للدخول إلى الإنترنـت، يجري الربط بينك كمالك للخلوي مع عملية البحث، على الرغم من أن المواقع الشبكيّة ربما تجهل ذلك.

مجاني ومريح

تشـكّل الرقابـة نموذج الأعـمال التجاريّة على الإنترنت، لسـببين رئيسـين: ميل النـاس إلى المجـاني، وانجذابهـم أيضـاً إلى ما هو مريـح. على الرغم مـن ذلك، تبقى حقيقـة أن النـاس ليـس لديهم خيار فعـليّ. وتتمثّل الحـال في أنّه إمـا الرقابة أو عدم

الحصول على شيء؛ ولكون الرقابة غير منظورة، وهو أمر مريح، فليس عليك التفكير بها. وغدت الأمور كلها ممكنة لأن القانون الأميركي لم يتطوّر ليواكب المتغيّرات في ممارسة الأعمال التجاريّة.

قبل العام 1993، كانت الإنترنت غير تجاريّة بالمرّة، والمجاني هو العرف السائد على الشبكة. عندما وصلت بواكير الأعمال التجاريّة إلى الشبكة، ثار كثير من النقاش عن طريقة جعلها مدفوعة. وسرعان ما تبيّن أنّه، فيما عدا حالات استثنائيّة معزولة كالاستثمار المباشر والمواقع الإباحيّة جنسيّاً، لا يرغب الناس في دفع ولو قليل من المال مقابل الوصول إلى خدمات الشبكة[19]. وبما يشبه كثيراً نموذج الأعمال التجاريّة على التلفزيون، شكّلت الإعلانات النموذج الوحيد للحصول على مردود مجزٍ، ومكّنت الرقابة من جعل الإعلان مربحاً أكثر. وبات بإمكان المواقع الشبكيّة أن تفرض رسوماً أعلى على الإعلانات الموجّهة بصورة شخصيّة، من تلك التي تحصّلها مقابل البث العام للإعلانات. وعلى ذلك النحو، وصلنا إلى وضع تسود فيه نُظُم مجانيّة اسميّاً، وهي تجمع بياناتنا وتبيعها مقابل ما تقدّمه لنا من خدمات، ثم تقصفنا بالإعلانات.

يمثّل «المجاني» سعراً له طبيعة خاصة به[20]، كما أثبتت بحوثٌ عدّة أنّ الناس لا تتفاعل معه بصورة منطقيّة. إذ نميل إلى الإعلاء من قيمة ما هو مجاني. نضغط على آخرين كي يستخدموه. يطوّق المجاني حسّنا الطبيعي حيال مسألة التناسب بين الكلفة والمنفعة، ثم ينتهي الأمر بالناس إلى بيع بياناتهم الشخصيّة بأقل من قيمتها.

يتضاعف ذلك الميل إلى تقليل قيمة الخصوصيّة لأن الشركات تسعى إلى التأكّد من ألا تكون أمراً بارزاً عند جمهور المستخدمين. عندما تدخل إلى «فيسبوك»، أنت لا تفكر في كمية المعلومات الشخصيّة التي تقدّم إلى الشركة، بل تفكر في أنك تتحادث مع أصدقائك. عندما تستيقظ صباحاً، أنت لا تفكر في أنك بصدد السماح لحفنة من الشركات بأنّ تتبعك طيلة النهار، بل تكتفي بأن تدس الخلوي في جيبك.

وتتجسّد النتيجة في أنّ شركات الإنترنت تستطيع تحسين عروضها للشراة الفعليّين، بتهوين قيمة خصوصيّة المستخدم. يمارس موقع «فيسبوك» ذلك الأمر منهجيّاً منذ سنوات[21]، بواسطة تحديثه بانتظام سياسته في الخصوصيّة بهدف الحصول على مزيد من الوصول إلى بياناتك، وإعطائك مقداراً أقل من الخصوصيّة. وكذلك بدّل «فيسبوك» سياسته حيال الأمور الأساسيّة في خلفيّة الإعدادات[22]، بما يمكّن مزيداً من الناس من رؤية اسمك، وصورتك، وتدويناتك، والصور التي تضعها على صفحتك، والأشياء التي ضغطت زر «لايك» عليها وما إلى ذلك. فعل محرّك البحث «غوغل» أموراً مشابهة كثيرة[23]. ففي العام 2012، أعلن «غوغل» تغييراً أساسيّاً قوامه أنه سيصنع مجموعة معلومات موحّدة يربط فيها بياناتك التي تأتيه من عمليات التفتيش، بريد «جي ميل»، موقع «يوتيوب» (الذي اشتراه «غوغل»)، «غوغل+» وغيرها.

في ذلك المضمار، تكاد شركة «آبل» أن تكون استثناءً[24]. إذ تتعامل الشركة مع أسواق السلع الاستهلاكيّة، ولكن على الرغم من أنها تستطيع التجسّس على البريد الإلكتروني في قاعدة بياناتها المُسمّاة «آي كلاود» (iCloud)، والرسائل النصيّة، والمفكرات، ودفاتر العناوين، والصور؛ فإنها تحجم عن ذلك الأمر. وتستعمل المعلومات عن عمليات الشراء في مخزنها الشبكي «آي تيونز» (iTunes) [25]، وبصورة حصريّة، لمجرد اقتراح أغانٍ أخرى وأشرطة فيديو مختلفة ربما رغب المستخدم في شرائها. ومنذ العام 2014، شرعت في استخدام ذلك الملمح باعتباره صفة تنافسيّة مميّزة لها في السوق.

تشكّل الراحة السبب الثاني في كوننا نسلّم طوعيّاً بياناتنا الشخصيّة جداً إلى مصالح الشركات، ونصبر على تحوّلنا أشياء تخضع لرقابتها. ومثلما أقول تكراراً، إنّ الخدمات المستندة إلى الرقابة هي مفيدة وقيّمة. إذ نسعد لكوننا قادرين على الوصول إلى دفاتر العناوين، والمذكرات، والصور، والوثائق، والأشياء الأخرى كافة، أينما كنّا وبواسطة أي جهاز يكون متاحاً لنا. يعجبنا وجود خدمات كمحرّكي البحث

«سيري» (Siri) و«غوغل ناو» (Google Now)، وهما يتألّقان في عملهما كلما كان بحوزتهما أطنان من المعلومات عنك. تسهّل تطبيقات شبكات الـ«سوشال ميديا» مسألة الاتّصال مع أصدقائنا. تزداد فعاليّة أداء تطبيقات خلوية كـ«خرائط غوغل» و«ييلب» و«ويزر» (Weather) و«أوبر»، كلما زادت معرفتها بالأمكنة التي نكون فيها. ويبدو سماحنا لتطبيقات كـ«بوكيت» (Pocket) و«إنستابايبر» (Instapaper)، بمعرفة عاداتنا في المطالعة، ثمناً قليلاً مقابل الحصول على معظم ما نرغب في قراءته متجمّعاً في المكان نفسه. وربما نسرّ أيضاً عندما تصلنا إعلانات موجّهة تحديداً إلى ما نهتم به. إنّ المكاسب المتحصلة من الرقابة في تلك التطبيقات وغيرها، هي فعليّة ومؤثّرة.

وعلى نحو خاص، لا نمانع أن تجمع الشركات معلومات عنا وتستخدمها في تحسين خدماتها كي تكون خدومة أكثر بالنسبة لنا. ويفسر ذلك أن شكاوى الناس بشأن رقابة الشركات، لا تتضمّن غالباً توصيات بشأن موقع «آمازون». فبصورة مستمرة، يقدّم لنا ذلك الموقع نصائح تستند إلى ما نشتريه، وما اشتريناه ماضياً، وما اشتراه آخرون أيضاً. وبذا، يستعمل «آمازون» بياناتك بطريقة تجميعها نفسها، ويكون فائق الشفافيّة مع المستخدم في ذلك الشأن. إنها تجارة ضخمة لـ«آمازون»، وتلقى قبولاً واسعاً لدى الجمهور[26]. ولكن، يبدأ الناس بالشكوى عندما تباع بياناتهم وتشترى وتستعمل، من دون علمهم وبلا إذن منهم.

صناعة اسمها: سماسرة المعلومات

ترجع رقابة الزبائن إلى عهود سابقة على عصر الإنترنت بكثير. فقبل ذلك العصر، وُجِدَت 4 تيّارات رئيسة للرقابة. تأتّى التيار الأول من احتفاظ الشركات بسجلات عن زبائنها. كان المثل على ذلك هو شركة للإمداد بمتطلبات التصنيع تحتفظ بسجلات عن طلبيات زبائنها من المؤسّسات، ومن هم الذين يقومون بالطلبيّات فعليّاً. كان ذلك عهداً تتذكّر فيه شركة «نوردستروم» (Nordstrom)

للحياكـة، أحجام زبائنها ونوعيّة الخياطة التـي ينجذبون إليها، وتحتفظ فيه شركات الطـيران والفنادق بسـجلات عن زبائنها الدائمين. بالنتيجـة، تطوّرت تلك الأمور كلهـا لتصنـع قاعـدة بيانـات تمكّن الـشركات من تتبع مسـارات مبيعاتهـا بداية من الطلبيّـة الأولى وانتهـاءً بالـشراء فعليّاً، وبطاقات ولاء الزبائن التي تمنح حسـومات للمسـتهلك لكن غاياتها الفعليّة كانت تقصّي مشـترياتهم. وحـاضراً، تمنح شركات كثيرة نُظُماً تعرف باسـم «إدارة العلاقة مع الزبون» (اختصاراً، «سي آر إم» CRM)، إلى المؤسّسات من الأحجام كافة.

جـاء التيار الثاني من الرقابة التقليدية، بواسـطة التسـويق المباشر. شـكّل البريد الورقي واسـطتها، فيـما تمثّل الهدف في إمـداد الشركات بقوائم لأسـماء من يرغبون في تلقي بريد تسـويقي، وعدم تبديد الرسـائل على أناس لا يرغبون في تلقيها. كانت تلك العمليّة تقريبيّة بالضرورة؛ لأنها استندت إلى أشياء كالمعلومات الديموغرافيّة، أو اشتراكات المجلات، أو قوائم الزبائن من شركات السلع المختلفة.

وأتـى التيـار الثالـث مـن مكاتـب الائتـمان. إذ دأبت تلـك الـشركات على جمع معلومات ائتمانيّة عن الناس، ثم بيع المعلومات إلى بنوك تريد اتّخاذ قرار بشأن إعطاء زبائنها قروضاً، وكذلك معدلات الفوائد عليها. ونسـبيّاً، كان ذلك نوعاً مكلفاً من عمليّـات جمـع المعلومات الشـخصيّة، ولا تكون مجدية إلا إذا تعلـق الأمر بكميات كبيرة من النقود: إعطاء بطاقات ائتمان، والسـماح لشخص ما باستئجار شقة وما إلى ذلك.

جـاء التيار الرابع مـن الحكومات. وتكوّن من السـجلات الحكوميّـة بأنواعها: شـهادات الميـلاد والوفاة، سـجلات رُخَص السـواقة، قوائم الناخبين، الشـهادات والرُخَص المتنوّعة وهكذا دواليك. وباطّراد، صار باسـتطاعة الشركات أن تشـتري تلك البيانات العامة، أو تنزلها بواسطة الإنترنت من المواقع الحكوميّة[27].

جمعت مكاتب الائتمان وشركات التسويق المباشر تلك التيارات الأربعة كي تصبح شركات لسماسرة المعلومات، التي هي حالها حاضراً على غرار شركة «آكزيوم»[28]. تشتري تلك الشركات[29] بياناتك من الشركات التي تتعامل معها، ثم تربطها مع معلومات أخرى عنك، ثم تبيع البيانات الناتجة عن تلك العمليات إلى شركات تريد معرفة مزيدٍ من المعلومات عنك. وركبت شركات سماسرة المعلومات موجات الأتمتة والانتقال إلى عصر الكومبيوتر. وكلما زادت كمية المعلومات التي تنتجها أنت بنفسك، تمكنت تلك الشركات من جمع مزيد من البيانات، مع رفع قدرتها على صنع ملف شخصي دقيق عنك[30].

يثير الدهشة حقاً ما تتمتع به معلومات سماسرة البيانات من السعة والعمق[31]. إذ يجمع أولئك السماسرة معلومات ديموغرافيّة كالأسماء، العناوين، أرقام الهاتف، عناوين البريد الإلكتروني، النوع الجنسي، العمر، الحال العائليّة، وجود أطفال في الأسرة، المستوى التعليمي، المهنة، مستوى الدخل، الانتماء السياسي، السيارات، ومعلومات عن المنازل والملكيات وغيرها. ويجمعون أيضاً قوائم عن مشترياتك، وتاريخ الشراء وطريقة الدفع.

وكذلك يتتبعون حالات الطلاق، والوفيات والأمراض في عائلتك. ويجمعون كل شيء عما تفعله على الإنترنت[32].

ويستخدم سماسرة البيانات المعلومات عنك كي يصنّفوك في فئات قابلة للتسويق[33]. هل تريد قوائم عمن يندرجون في فئات «وارث محتمل» أو «بالغ يعيل أبويه العجوزين»، أو عناوين الأسر التي «تركّز على مرض السكري» أو «حاجات المسنين»؟ تستطيع شركة «آكزيكوم» إمدادك بتلك القوائم كلها[34]. باعت شركة «إنفويو إس إيه» (InfoUSA) قوائم عن «مسنين قيد المعاناة» و«مسنين تسهل مخادعتهم»[35]. في 2011، باعت إحدى شركات سماسرة البيانات، اسمها «تلتراك» (Teletrack)، قوائم عمن تقدموا بطلبات عن مكوّنات ائتمانيّة غير مألوفة

كقروض الدفع اليومي، إلى شركات كانت تسعى لعقد صفقات مالية سيّئة مع مثل أولئك الأشخاص. في 2012، باعت شركة السمسرة «إيكويفاكس» (Equifax) قوائم المتخلفين عن دفع أقساط رهوناتهم، لشركات تقدّم ديوناً منخفضة الفائدة. ولأن ذلك الأمر تعلّق ببيانات ماليّة، فرضت «المحكمة الفيدراليّة للتجارة» غرامات ماليّة على «إيكويفاكس» والشركات التي اشترت قوائمها أيضاً[36]. في ما عدا ذلك، بدت الأمور الأخرى كأنها تسير بعدالة تامة.

الإعلانات الشخصيّة

نستعمل نُظُماً تتجسّس علينا لقاء الحصول على خدمات[37]. وحاضراً، تسير أمور الإنترنت على هذا النحو. إذا كان شيء ما مجانياً، فأنت لست المستهلك[38]؛ بالأحرى أنت المُنتَج. ووفق تعبير آل غور، المرشح السابق للرئاسة في أميركا: «لدينا اقتصاد يبحث عن طرائد»[39].

ودوماً، عانت الإعلانات من مشكلة أن معظم من يشاهدونها لا يهتمّون بالمنتجات التي تعرضها. يعدُّ تبديداً أن تقدّم إعلاناً عن البيرة لمن لا يتناولها. ينال التبديد معظم الإعلانات عن السيارات، إلا إذا كنتَ في سوق للسيّارات. ولكن، مع استحالة توجيه الإعلانات بطريقة إفرادية، تصرّفت الشركات بأحسن الطرق بالبيانات الموجودة لديها. إذ قسَّمت الناس جغرافيّاً، ووضَعَت أفضل التخمينات عن المجلات والبرامج التلفزيونيّة الأكثر قدرة على جذب مستهلكين محتملين. لقد تتبعوا السكان بعمومهم، أو بتقسيمهم إلى مجموعات ديموغرافيّة كبرى. اتّسمت تلك الأمور كلها بغياب الفعاليّة. ثمة قول مشهور غالباً ما ينسب إلى جون وانامايكر، قطب مبيعات التجزئة: «أعلم أن نصف إعلاناتي هي تبديد تام. وتكمن المشكلة في أنني لا أعرف أي نصف منها هو كذلك»[40].

تملك الرقابة الشاملة الكليّة القدرة إمكانيّة تغيير ذلك الأمر. إذا كنت تعرف بالضبط من يرغب في شراء جزّازة للعشب أو من يقلق بشأن ضعف الانتصاب[41]،

يغدو باستطاعتك توجيه إعلانك إلى الشخص المناسب في الوقت المناسب، مع عدم تبديد أي شيء. (فعليّاً، تستخدم شركة لرعاية الحدائق[42] تعمل على مستوى أميركا كلها صوراً جويّة كي تروّج لإعلاناتها بشكل أفضل). وإذا علمت التفاصيل الكاملة عن مستهلك محتمل- بما فيها نوع الحجج التي تقنعه، وأنواع الصور المرغوبة لديه- تغدو إعلاناتك أشد فعاليّة.

ينطبق الوصف عينه على الإعلان السياسي، بل غيّر فعليّاً طريقة إدارة الحملات السياسيّة[43]. استخدم باراك أوباما «البيانات الضخمة» و«الإعلان الشخصي» في حملتيه الرئاسيتين عامي 2008 و2012 [44]، ويسير على منواله مرشحون من الطيف السياسي بأكمله. تستخدم تلك البيانات في توجيه جهود التمويل والرسائل السياسيّة الفردية[45]، والتأكّد من ذهابك إلى صناديق الاقتراع يوم الانتخاب؛ مع افتراض أن قاعدة البيانات تشير إلى أنك ستصوت للمرشح المناسب لأصحابها.

تكتظ بيانات الرقابة التجارية بأخطاء متنوّعة[46]، لكنها تكون مفيدة[47] حتى عندما لا تكون دقيقة تماماً. فحتى لو وصل بك الأمر إلى إيصال ثلث إعلاناتك إلى أشخاص لا يجدي استهدافهم بها، تكون قد أدرت حملة إعلانية فعّالة حقاً. لا يكمن وجه الأهمية في الدقة الكاملة لتوجيه الإعلانات، بل في كون المعلومات أصبحت أفضل بكثير مما كانته في الماضي[48].

في العام 2013 مثلاً، استطاع بحّاثة أن يحدّدوا الأمكنة الجغرافيّة لأشخاص يستعملون «تويتر»، بتحليل تشابهاتهم مع مستخدمين آخرين لـ «تويتر»[49]. لم يكن معدل الدقة مرتفعاً لديهم- إذ بلغت 58 ٪ عند تحديد المدينة التي كان فيها المستخدمون- لكن تلك النسبة تعدُّ أكثر من كافية بالنسبة لعدد كبير من شركات الإعلانات التجاريّة.

على الرغم من ذلك، تتوافر أدلة كثيرة على أن الإعلانات المستندة إلى الرقابة تُباع بسهولة[50]. هناك قيمة لإبراز الإعلانات إلى أناس يرغبون بها، خصوصاً عندما

تصلهـم في اللحظة التي يكونون فيها بصدد اتخّاذ قرار الشراء. يحاول «غوغل» فعل ذلك بالضبط بواسـطة خدمـة «آد ووردز» (Adwords) التي تضع الإعلانات قرب نتائـج عمليـات البحـث. ويحاول الأمـر عينه باعـة التجزئة على الإنترنت بواسـطة الإعلانات التي تقول «الذين اشـتروا هذا الشيء، اشتروا تلك الأشياء أيضاً». لكن تلك الأشياء تستند إلى قليل من الرقابة.

ليس واضحاً ما هي كمية المعلومات التي تعدُّ كافية. هناك أهمية لمعرفة معلومات شـخصيّة عامـة عن الناس: مثليو الجنـس، المقبلون على الـزواج، الذين يفكرون في قضاء عطلة في مناطق دافئة، الذين لديهم مسـتوى معين من الدخل. وتعطي شركة للسـيارات قيمـة كبيرة لمعلومـة تفيدها بأنك ترغب في سـيارة عائليّة وليس سـيارة بسـقف متحرّك، لكنها لا تقيـم وزناً كبيراً لمعرفة تفضيلك أن تكون السـيارة زرقاء أو خـضراء. وكذلـك الحال للمعلومـة التي تقول إن لديك طفلـين، أحدهما ما زال بحاجـة إلى كرسي طفـل على المقعد الخلفـي، أو أن أحد الطفلين قـضى أثناء حادث تحطّـم سـيارة[51]. صحيح أن وكيـل البيع سـيحاول إقناعك بشراء سـيارة أكبر في الحـال الأولى (لديـك طفلان)، وبمعايير السـلامة في الثانية (طفـل قضى في حادث سـيارة)، لكـن الفـارق في العائـدات سـيكون ضئيلاً باسـتمرار. وكذلـك ربما يثير الإعلان المشخصن بدقة نوعاً من الريبة، ما يهدد بانصراف الزبون عن الشراء[52].

في هـذا المضـمار، يفيد تذكّـر مفهوم يأتي من عـوالم الروبوت. إذ نرتـاح للتعامل مع الروبوتات التي تبدو لنا كروبوتات منذ النظرة الأولى، وكذلك تلك التي تشـبه البشر تماماً. لكننا لا نشعر بالراحة مع روبوت يشبه الناس كثيراً، لكنه لا يكون بشريّاً تماماً. أشـار عالم الروبوت الياباني ماسـاهيرو موري إلى تلك الظاهرة باسم «الوادي غـير الحاذق»[53]. ولفتت سـارة دبليو. واطسـون، وهي من نقّـاد التكنولوجيا، إلى وجـود ظاهـرة مماثلـة في عـالم الإعـلان. إذ يرتاح النـاس إلى إعلانات تحمـل طابعاً شخصيّاً مواربأً[54]، وكذلك الحال مع الإعلان الذي يكون طابعه الشخصي مرهفاً

وغـير ملموس، لكنهم ينفرون من إعلان «مريب» نسـبيّاً فيه ما يوحي بأنه يتلاعب بهم أو يكون غير متطابق مع نظرتهم لأنفسهم.

سـوف يتغيّر ذلك كله مع الزمن، عندما نعتاد على الإعلان الشـخصي. الحال أن تعريف «المريب» نسبي وسيّال[55]، ويعتمد كثيراً على مدى ألفتنا مع التكنولوجيات موضـع البحث[56]. حـاضراً، تكون مريبة تلك الإعلانات التـي تتبعنا أثناء تجوالنا بواسـطة الإنترنت[57]. ويمكن للمريب أن يصحّح نفسـه بنفسـه. يملك «غوغل» تاريخاً طويـلاً ومعقـداً مـع الإعلانات التي لا يسـمح لها بـأن تترافق مـع عمليات البحـث عليـه؛ لأن مسـتخدمين وجـدوا أنّ بعض أنـواع الإعلانات تثير إحساسـاً بالريبة لديهم. وتسـمح شركات أخرى للمسـتخدمين بالنقر عـلى وصلة إلكترونيّة تفيـد في تعريفهـم بسـبب ملاحقتهـم من قِبَـل إعلان معـين[58]. ويهـدف ذلك إلى جعلهم أكثر ألفة مع عملية الإعلان الشخصي.

مـن الناحيـة الثانية، تكتفـي شركات بإخفاء الأمر. بعد القصـة التي وردت آنفاً عـن تمكّـن شركة «تارغِت» مـن التعرّف إلى حمـل مراهقة كانت تخفيه عـن أبيها(*)، غيّرت الشركة أسـلوب إرسـال الإعلانات الشـخصيّة إلى الناس. إذ لم تتوقّف عن إرسـال إعلانات للنسـاء اللواتي تخمّن أنهن حوامل، لكنها دسّـتها ضمن إعلانات أكثر عموميّة. لم تشـعر اللواتي وصلتهن تلك الإعلانات بواسـطة الـ«إيميل» أنهن مستهدفات على نحو شخصي، لذا أحسسن بريبة أقل حيالها[59].

في الوقـت عينه، يؤدّي تكاثر الإعلانات حولنـا إلى التقليل من قيمة الإعلانات الفرديّة، لسـببين على الأقل: أولاً، مع تشبّع عالمنا بالإعلانات، تتدنى قيمة الإعلان الموجّـه إلى كل فـرد منا. ويرجع ذلك إلى أن كمية النقـود التي ننفقها لا تتغيّر. مثلاً، تتصارع شركات السيّارات كلها على الربح المتأتي من السيارة الواحدة التي تشتريها.

(*) راجع الفصل الثالث.

إذا رأيت عشرات أضعاف الإعلانات، يكون لكل منها عُشر القيمة؛ لأنك لن تشتري في ختام المطاف سوى سيّارة واحدة.

ثانياً، من السهل علينا تماماً إبعاد الإعلانات عنّا. منذ رواج أشرطة الفيديو التقليديّة في منتصف السبعينيات من القرن العشرين، تنبّه المعلنون إلى أهمية الشكل الذي تبدو عليه إعلاناتهم عندما يستخدم الناس زر «إلى الأمام بسرعة»، كي يقفزوا عن مشاهدتها. خاضت شركات الإعلانات الشبكيّة معركة أكثر تعقيداً بهدف الاستحواذ على اهتمامنا.

في البداية كانت تلك الإعلانات مجرد لوحات تظهر في أعلى صفحات الإنترنت. وعندما تعلّمنا أن نتجاهلها، شرعت في تبني طريقة الومض مع إظهار شرائط الفيديو الرقميّة. وحاضراً، صارت الإعلانات متداخلة كثيراً مع ما نريد قراءته، ما يلجئنا إلى تعمّد إبعادهم عن أبصارنا. ويقدّر أن ما يزيد على 50 مليون شخص، وضعوا برنامج «آدبلوك بلاس» (AdBlock Plus) [60] الذي يصدّ الإعلانات في محرّكات البحث.

وبالنتيجة، تنخفض قيمة الإعلان الشبكي المفرد باطّراد[61]، على الرغم من الارتفاع المستمر في تكلفة الإعلان بواسطة الإنترنت. ووفقاً لذلك، تدنّت بسرعة قيمة بياناتنا بالنسبة للمعلنين. قبل بضع سنوات، كان الملف الشخصي التفصيلي عن كل فرد يحوز قيمة كبيرة، وحاضراً يحوز عدد كبير من الشركات وسماسرة البيانات تلك المعلومات، ما جعلها سلعة عاديّة[62]. في سياق تحليل تقارير ماليّة في 2013، ورد أن قيمة البيانات عن الفرد تصل إلى 42 دولاراً سنويّاً على محرّك البحث «غوغل»[63]، لكنها مجرد 6 دولارات في «فيسبوك»، وشبكة «لينكدن» (LinkedIn) المهنيّة ومتصفّح «ياهوو» (Yahoo!). وللسبب عينه، لا يكف موقعا «غوغل» و«فيسبوك» عن رفع لواقطهما. إذ يحتاجان إلى مزيد ومزيد من المعلومات عنا كي يبيعاها للمعلنين، وبالتالي ينأيان بنفسيهما عن المنافسة.

من المحتمل أننا وصلنا نقطة الذروة[64]، ما يعني أن الربحيّة من مردود الإعلانات سوف تشرع في الانحدار، ما يوصلها إلى وضع تكون فيه غير قادرة على الاستمرار كنموذج وحيد للعمل. لا أظن أن أحداً يعرف كيف ستبدو عليه الإنترنت إذا انفجرت فقاعة إعلاناتها[65]، وأضحى التسويق بواسطة الإعلانات المستندة إلى الرقابة غير مجدٍ، واضطرت شركات الإنترنت إلى العودة للأسلوب القديم في الأعمال: أن تفرض رسوماً على مستخدميها.

قوة الوسطاء الجدد

تمثّلت إحدى «الكليشيهات» المبكّرة للإنترنت في أنها سوف تنهي الشركات الوسيطة[66]. لن تعتمد على الصحف التي تستعرض الأخبار اليوميّة وتقدّمها لك في حزمة ورقيّة قابلة للقراءة بسهولة. فعلى الإنترنت، تستطيع أن تصمّم الصحيفة التي ترغب فيها، وتأخذ نتفاً من هنا وهناك كي تصنع ما تريده تحديداً. وعلى نحو مماثل، لن تعتمد على المخازن الكبرى في البيع والتسوّق، سوف يعمل موقع «إي باي» (eBay) المختص بالتجارة الإلكترونيّة على ربط الباعة بالشراة مباشرة[67]. وسارت الأمور على النحو نفسه بالنسبة للترويج والتوزيع في الموسيقى[68] وتذاكر الطيران[69]، وفي بعض الأحيان، الإعلانات التجاريّة[70]. ساد اعتقاد بأن النماذج السابقة في الأعمال اعتمدت على قدامى «حُرّاس البوابات»(*)، والإنترنت غيّرت تلك الآليّات كلها.

يصح الأمر حاضراً بأكثر مما كانه قبلاً. إذ يتيح موقع «إربن بي» للأفراد التنافس مع الفنادق التقليديّة. ويسهّل موقع «تاسك رابت» الاتّصال بين الأشخاص الذين يريدون القيام بأعمال غير مستساغة مع الناس الذين يسعون إلى العثور على من ينفذ لهم أعمالاً غير مستساغة. وتلغي مواقع «إي باي» و«إيتساي» و«كافيه-برس» الحاجة إلى أسواق بيع الأشياء المستعملة. يتجاوز موقعي «زيلو» و«ريدفن»

(*) إشارة إلى الدور الذي يؤديه الوسطاء، سواء أكانوا أفراداً أم شركات.

أعمال السماسرة العقاريّين، وكذلك يفعل موقع «إي ترايد» بالنسبة لمستشاري الاستثمارات، وينطبق ذلك على ما يفعله موقع «يوتيوب» بشبكات التلفزة. ويلغي موقع «كريغ ليست» الحاجة إلى التحقيقات الصحافيّة، ويفعل موقعا «هوت واير» و«ترافيلوسيتي» الأمر عينه بالنسبة لوكلاء السفر.

ربما نجحت الشركات الشبكيّة الجديدة في كسر مراكز القوة التقليديّة للمتاجر الكبرى، والصحف، وشركات التاكسي؛ لكن تحكّمها في سريان المعلومات بين الشراة والباعة أوصلها إلى تأديتها هي نفسها دور الوسطاء الأقوياء. وأمام ناظرينا، بات السوق مساحة لمعركة بين الوسطاء القدماء والجدد. إذ تتصارع «آبل» ومخزنها «آي تيونز» مع الصناعة التقليدية للموسيقى، ويتواجه «آمازون» مع دور النشر التقليدية، و«أوبر» (Uber) مع شركات سيارات الأجرة. ويكسب الوسطاء الشبكيون الجدد تلك المعركة باستمرار.

عبرّ إريك شميدت، المدير التنفيذي لـ«غوغل»، عن ذلك بوضوح قائلاً[71]:
«نعتقد أن منصات التقنيّات الحديثة كـ «غوغل» و«فيسبوك» و«آمازون» و«آبل»، هي أشد قوّة مما يعتقد كثيرون... وما يمنحهم تلك القوّة قدرتهم على النمو، تحديداً قدرتهم على رفع كمية أعمالهم بأضعاف مضاعفة، بسهولة وسرعة فائقة. لا شيء، ربما ما عدا الفيروسات البيولوجيّة، يستطيع فعل ذلك بسرعة تلك المنصّات التكنولوجيّة وكفاءتها وقوّتها، وهو أيضاً ما يجعل من يصنعون تلك المنصات ويديرونها ويستعملونها، أقوياء تماماً».

تشير كلمات شميدت إلى الطبيعة الاحتكاريّة المتأصّلة في الوسطاء الشبكيّين الجدد. هناك مجموعة متنوّعة من التأثيرات الاقتصاديّة التي تكافئ من ينطلق أولاً[72]، وتعاقب من يدخل المنافسة متأخّراً، وتربط الناس بالشبكات الأكثر ضخامة، ما يجعل من الصعب عليهم الانتقال إلى نُظُم منافِسَة. ونتيجة لذلك، يحوز

أولئك الوسطاء الشبكيّون الجدد قوّة أكبر مما امتلكه الوسطاء القدماء الذين حلّ الجدد بديلاً منهم.

إذ يتحكّم «غوغل» بثلثي سوق عمليات البحث على الإنترنت[73]. وأنشأ ثلاثة أرباع مستخدمي الإنترنت حسابات لهم على «فيسبوك»[74]. ويتحكّم موقع «آمازون» بقرابة 30 ٪ من سوق الكتب في الولايات المتّحدة[75]، وتحوز شركة «كومكاست» قرابة 25 ٪ من سوق الاتّصال بالإنترنت[76]، بواسطة الموجات العريضة النطاق [«برودباند» (Broad Band)]. تملك تلك الشركات قوّة هائلة، وتتحكّم بنا ببساطة استناداً إلى مستوياتها الاقتصاديّة.

تجمع تلك الشركات كلها بياناتنا كي تزيد من هيمنتها على السوق وربحيتها في الأعمال. عندما انطلق موقع «إي باي» للتجارة الإلكترونيّة، كان من السهل على الشراة والباعة أن يتحاوروا خارج نظام «إي باي»؛ لأن عناوين البريد الإلكتروني للأفراد كانت متاحة للعموم.

في العام 2001، شرع «إي باي» في إخفاء عناوين البريد الإلكتروني[77]، وفي 2011، حظر وضع عناوين البريد الإلكتروني والوصلات الإلكترونيّة في القوائم[78]، وفي 2012، حظرت تلك المعلومات في التراسل بين مستخدم وآخر[79]. خدمت تلك التحرّكات كلها أن يصبح «إي باي» وسيطاً قويّاً بتصعيبه عمليات إنشاء صلات بين الباعة والشراة داخل نظام «إي باي»، ثم نقلها إلى خارجه.

وباطّراد، تستخدم الشركات قوّتها للتأثير في مستخدميها والتلاعب بهم. تبذل المواقع الشبكيّة التي تستفيد من الإعلانات جهوداً مكثّفة للتأكّد من قضائك أطول وقت ممكن عليها[80]، بتعديل محتوياتها كي تصبح جذّابة إلى حدّ إدمانها. وتلجأ القلّة من المواقع التي تسمح لك بالخروج من إعلاناتها الخاصة إلى تصعيب عملية

الوصـول إلى ذلـك الخيـار[81]. وبمجـرد أن تتمكن الـشركات من المـزج بين تلك التقنيّات والمعلومات الشخصيّة، تضحي النتائج أعمق غوراً وأشد خفاءً وتراكميّة.

لا تعتمـد علاقاتنـا مـع مجموعـة كبـيرة مـن شركات الإنترنـت عـلى النمـوذج التقليـدي لعلاقـة الشركة بالزبون. ويرجع ذلك أساسـاً إلى أننا لسـنا مجـرد زبائن. بالأحـرى، نحـن منتجـات تبيعها تلك الـشركات إلى زبائنها *الحقيقيّـين*. إنّها أقرب إلى العلاقـات الإقطاعيّـة من كونهـا علاقات تجاريّـة[82]. تشـبه شركات الإنترنت السـادة الإقطاعيّين، ونحن رعاياهم توابعهم وفلاحيهم، بل نكون- في يوم سيئ- خَدَمَهم. نحن مزارعون مسـتأجرون بالنسـبة لتلك الشركات، إذ نعمل في أراضيها وننتج معلومات تتولى بيعها للحصول على أرباح.

نعم، تمثّل الكلمات السـابقة مجازاً؛ لكن الأمور تكون كذلك غالباً. أقسـم بعض الناس يمين الولاء لـ «غوغل». إذ ينشؤون حساباً على بريد «جي ميل» الإلكتروني، ويسـتخدمون «وثائق غوغـل» و«مفكرة غوغل»، كما يحملـون هواتف تعمل بنظام الـ «آندرويـد» الـذي صنعـه «غوغـل». وأقسـم آخرون يمـين الـولاء لـ «آبل». إذ يملكون حواسـيب مـن نوع «ماك- آبـل»، وهواتف «آي فون»، وألـواح «آي باد» الإلكترونيّة، ويسـمحون لموقع «آي كلاود» بالاحتفاظ بنسـخ عن أشـيائهم كلها، مع تحديثها كلما جدّ جديد. وما زال بعضنا يسـمح لـ «مايكروسوفت» بتولي الأمور كلها. وهجر شـطر كبير منا البريد الإلكتروني ليتّكل كلياً على «فيسـبوك»، و«تويتر» و«إنسـتغرام». ربما نفضّل سـيّداً إقطاعيّـاً على غيره. ربما نـوّزع ولاءنا على عدد من تلـك الـشركات، أو نثابر على تجنّب شركـة ننفر منها. بصرف النظـر عن ذلك كله، بات من الصعب عدم الولاء على الأقل لواحد من أولئك السادة.

في نهايـة المطاف، يحصـل الزبائن على منافع كثيرة من الولاء لسـادة الإقطاعيّين. فببسـاطة، من الأسـهل والأكثر مأمونيّة أن يتولى شـخص آخر حفظ بياناتنا وإدارة أجهزتنا. إذ نرغب أن يتولى شـخص آخر العناية بإعـدادات أجهزتنا وضبطها[83]،

وإدارة البرامج فيها، وتخزين المعلومات عليها. ونرغب في الوصول إلى بريدنا الإلكتروني من كل الأمكنة التي نكون فيها، ومن كل كومبيوتر يتوافر لنا؛ وكذلك نحب أن يكون «فيسبوك» بتصرفنا، فندخله من كل الأجهزة وفي الأمكنة كلها. ونريد أن تظهر التحديثات التي نضيفها على مفكراتنا، بأجهزتنا كلها. تتفوّق علينا المخازن الرقميّة الضخمة لـ «سُحُب المعلومات» في تخزين صورنا وملفّاتنا؛ وأدّت «آبل» عملاً عظيماً بأن حمت المخزن الرقمي لتطبيق «آي فون» من البرمجيات الخبيثة. نحب تلقي تحديثات أمنية لحماية أجهزتنا، والاحتفاظ بنسخ أوتوماتيكيّة عن ملفاتنا؛ فالشركات أفضل منا تماماً في حماية أجهزتنا. ونشعر بالسعادة عندما نرى معلوماتنا كلها تظهر دفعة واحدة بكبسة زر، إذا فقدنا هاتفنا الذكي واشترينا آخر بديلاً عنه.

في العالم الجديد للحوسبة، لم يعد منتظراً منا أن ندير بيئة معلوماتنا الإلكترونيّة. نضع ثقتنا بأن يحسن السادة الإقطاعيّون معاملتنا ويحمونا من الأذى. تنجم تلك الأمور كلها من مسارين في التكنولوجيا:

يتمثّل المسار الأول في صعود تقنيّة «حوسبة السحاب» (Cloud Computing) [84]. وبصورة أساسيّة، تفترض تلك التقنيّة بأن المعلومات لم تعد تخزّن وتدار من أجهزتنا الخاصة؛ بل تحدث الأمور كلها في خوادم ضخمة تملكها مختلف الشركات المعلوماتيّة. النتيجة؟ نفقد السيطرة على معلوماتنا. تدخل تلك الشركات على معلوماتنا وبياناتنا- يشمل ذلك المحتوى و«البيانات الوصفيّة» معاً- خدمة لأي هدف ربحي تريده. وبحرص، صاغت الشركات بنود الخدمة، وهي تملي أنواع البيانات التي نستطيع تخزينها على نُظُم الشركات، ما يمكّنها من حذف حساباتنا بأكملها إذا ارتأت أنه يخالف تلك البنود. وتقدّم معلوماتنا إلى جهات إنفاذ القانون، من دون معرفتنا ولا موافقتنا[85]. أسوأ من ذلك، ثمة إمكان لأن تخزّن بياناتنا في كومبيوترات موجودة في بلاد لا تتمتع بقوانين قويّة لحمايتها.

يتمثّل الميل الثاني في صعود أجهزة المستخدم[86]، التي تستمر الجهات البائعة في إدارتها على نحو وثيق بعد بيعها. يشمل ذلك أجهزة «آي باد»، و«آي فون»، وهواتف الـ «آندرويد»، و«كيندل»، و«كروم بوكس» وغيرها. وبالنتيجة، لم نعد نسيطر على بيئة الحوسبة الإلكترونيّة، بأجهزتها وأدواتها وملفاتها. لقد سلّمنا إلى الشركات الزمام في كل ما نقدر أن نراه ونفعله ونستخدمه. تفرض شركة «آبل» قوانين[87] بشأن أنواع البرامج والتطبيقات التي يمكن وضعها على الأجهزة التي تعمل بنظام التشغيل «آي أو إس» الذي تملكه. وتستطيع أن تضع وثائقك الخاصة على جهاز «كيندل» للقراءة الإلكترونيّة، لكن مالكته «آمازون» تستطيع أن تحذف كتباً باعتها هي بنفسها لك. في العام 2009، حذفت «آمازون» أوتوماتيكيّاً نسخاً من رواية الكاتب جورج أورويل 1984 من أجهزة «كيندل»[88]؛ بسبب قضايا تتعلّق بالملكيّة الفكريّة. وبمرارة، أعرف أنه لم يعد ممكناً كتابة أعمال روائيّة مماثلة.

حتى النظامين الكبيرين في تشغيل الكومبيوترات، «ويندوز 08» (Windows 08) من «مايكروسوفت» و«يوزمايت» (Yosemite) من «آبل»، يسيران في ذلك الاتجاه عينه.

وتضغط كل من الشركتين على المستخدمين كي لا يشتروا سوى تطبيقات مجازة منها، ولا تباع سوى في مخازنها الرقميّة المركزيّة. ويتزايد الشبه بين كومبيوتراتنا وهواتفنا الذكيّة، مع كل تحديث لنُظُم التشغيل فيها.

لا يتعلق الأمر بالأجهزة وحدها. لم تعد طليق اليد في شراء أي برنامج ترغب فيه، وتضعه على كومبيوترك. وباطّراد، تتجه الشركات البائعة إلى تبني نموذج الاشتراك[89]- فعلت ذلك شركة «آدوبي» (Adobe) الشهيرة، عند إطلاقها سحابة «كرييتف كلاود» (Creative Cloud)[90] في 2013، التي تعطي الشركة البائعة سلطات كبيرة. لم تتخل «مايكروسوفت» كليّاً عن نظام البيع، لكنها جعلت الاشتراك في برنامج «أوفيس» مغرياً تماماً. ومن الصعب مقاومة ما يعرضه «أوفيس

365» (Office 365) لجهـة تخزيـن الوثائـق في «سـحابة المعلومـات» التـي تديرها «مايكروسوفت». تعمل الشركات على دفعنا في ذلك الاتجاه؛ لأنه يجعلنا ندر أرباحاً أكثر، كمستخدمين وزبائن.

في ظل القوانين السـارية حاضراً، تشـكّل الثقة خيارنا الوحيد. ليس ثمة قوانين منسـجمة أو قابلـة للتوقّع. لا سـلطة لنا عـلى أفعال تلك الشركات. لا أسـتطيع أن أتفـاوض بشـأن حق متصفّح «ياهـوو» في الوصول إلى صوري عـلى موقع «فليكر» (Flickr) المخصّـص لصـور الأفـراد. لا أسـتطيع تطلّـب مزيد من الحمايـة لشرائح العـروض الضوئيّـة الخاصـة بي، عندمـا أضعها على موقـع «بريـزي» (Prezi)، ولا قوائم الأشـياء الواجـب علي إنجازها عندمـا أضعها على موقع «تريلـو» (Trello). ولا أعرف حتى أسـماء الشركات التي أناط بهم مقدّمو خدمة «سحابة المعلومات»، إنجـاز البنية الإلكترونيّـة التحتيّة لتلك الخدمة. إذا حذفت تلـك الشركات بياناتي، لا أملـك حتـى الحق في طلب اسـترجاعها. لا خيـار لي في الأمر برمّتـه. وإذا قرّرت تـرك تلـك الخدمات، فالأرجح أنني لن أتمكن بسـهولة من أخـذ معلوماتي وبياناتي معي[91].

لاحـظ العالِم السـياسي هنـري فاريـل[92] أن «معظم حياتنا بات يجري بواسـطة الإنترنـت. وبقول آخر، صار معظـم حياتنا يجري بموجب قوانين تفرضها شركات القطاع الخاص، وهي لا تخضع لكثير من القوانين الحكوميّة ولا للمنافسـة التقليديّة في السوق الفعلي».

ثمـة دفاع يتكرّر حيال ذلك الأمـر، من نوع «الأعمال هي الأعمال». لا أحد مجبر على الانضمام إلى «فيسـبوك»، أو اسـتخدام عمليات البحث في «غوغل»، أو الشراء بواسـطة الــ «آي فون». ينخـرط المسـتخدمون طوعيّـاً في تلك العلاقات الشـبيهة بالإقطاعيّة، بسبب ضخامة ما يحصلون عليهم من خدمات لقاء ذلك. إذا لم يعجبهم الأمر، ليتوقفوا عنه.

تلـك النصيحـة ليسـت عمليّـة. ليس مـن المنطقـي القول للنـاس[93] إنـه إذا لم تعجبهـم عمليات جمع المعلومات والبيانات، سـيكون عليهم التوقف عن اسـتعمال البريد الإلكتروني، أو التسوّق بواسطة الإنترنت، أو استخدام «فيسبوك» أو امتلاك خلوي. لا أستطيع تخيّل أنه بمقدور الطلبة إنهاء مراحل تعليمهم بعد الآن، من دون اسـتعمال محرّكات البحث على الإنترنت أو موسـوعة «ويكيبيديـا»، ولا العثور على وظيفة بعد ذلك. إنّها أدوات الحياة الحديثة.

إنّها أدوات ضروريّة للمهن والحياة الاجتماعيّة. لا يمثّل الخروج منها خياراً قابلاً للحياة[94]، بالسنة لغالبيتنا؛ لكنها في معظم الأوقات تنتهك ما باتت أعرافاً فعليّة في الحياة المعاصرة.

وكذلك لا تمثّل المفاضلة بين مقدّمي الخدمات الإلكترونيّة اختياراً بين الرقابة أو عدمها، بل مجرد خيار للسيّد الذي يتجسّس عليك.

5

الرقابة والسيطرة الحكوميتان

ربما يصعب فهم المدى الكامل الذي تصله الرقابة الحكوميّة. سأركّز على حكومة الولايات المتّحدة، ليس لأنها المعتدي الأسوأ، بل لأننا نعرف شيئاً ما عن نشاطاتها؛ أساساً بفضل أعمال مشكورة لإدوارد سنودن.

تتميّز رقابة الأمن القومي في الولايات المتّحدة بأنّها مكينة سياسيّاً وقانونيّاً وتقنيّاً. كشفت وثائق سنودن[1] عن وجود ثلاثة برامج على الأقل، تملكها «وكالة الأمن القومي» لجمع المعلومات عن كل مستخدم لبريد «جي ميل». تستند تلك البرامج الثلاثة إلى ثلاث قدرات تقنيّة في التنصّت. وكذلك فإنّها تعتمد على ثلاث سلطات قانونيّة مختلفة، وتشتمل على تعاون ثلاث شركات مختلفة. تلك هي الصورة بشأن «جي ميل» وحده. وينطبق توصيف مشابه بصورة شبه مؤكّدة على الشركات الكبرى كافة التي تقدّم خدمة البريد الإلكتروني، سجلات الهواتف الخلوية، «البيانات المكانية» لتلك الهواتف، ومحادثات الإنترنت.

من أجل فهم دور الرقابة في الاستخبارات الأميركيّة، يجب فهم تاريخ مهمة «وكالة الأمن القومي» في التنصّت العالمي، والتغيير في طبيعة الجاسوسيّة. بسبب ذلك التاريخ، تمثّل «وكالة الأمن القومي» المنظّمة الرئيسة للتنصّت بالنسبة للحكومة الأميركيّة.

تأسّست «وكالة الأمن القومي» على يد الرئيس هنري ترومان في العام 1952[2]، الذي جمع الاستخبارات الأميركيّة لنظم الإشارة ونشاطات كسر الشيفرات ضمن منظّمة واحدة[3]. وكانت المنظّمة وما زالت جزءاً من الجيش الأميركي، واستهلّت عملها بوصفها منظّمة مختصة كليّاً في جمع المعلومات عن الاستخبارات الأجنبيّة.

وتزايدت أهمية تلك المنظّمة أثناء الحرب الباردة بين أميركا والاتّحاد السوفياتي. وحينها، كان التلصّص على الاتّحاد السوفياتي هو العرف السائد، وكانت الاستخبارات الإلكترونيّة جزءاً من ذلك، ثم زادت أهميّتها عندما صارت الأعمال كلها تجرى بواسطة الكومبيوتر، كما باتت الاتّصالات الإلكترونيّة أكثر شيوعاً. وزادت كمية المعلومات التي نجمعها مع تنامي قدراتنا وزيادة كمية الاتّصالات التي يجب تجميعها.

وعلى رغم عدم جدوى معظم تلك الأشياء، فإن بعضها كان مفيداً تماماً. وواضح تماماً أنّ الوصول إلى الأسرار عن الواقع[4]- على غرار ميّزات دبابة سوفياتيّة جديدة- هو أكثر سهولة من الوصول إلى ألغاز النوايا، من نوع الخطوة التالية التي يرغب الرئيس السوفياتي نيكيتا خروتشوف القيام بها. لكن، أولئك كانوا أعداءنا، وجمعنا كل شيء تمكّنا من جمعه عنهم.

كان من الواجب تقليص تلك المهمة المتفرّدة مع سقوط الشيوعيّة في أواخر الثمانينيات من القرن العشرين وبداية تسعينياته، كجزء من حصص السلام. لبرهة، سرى ذلك الأمر، وتنامت أهمية المهمة الأخرى لـ «وكالة الأمن القومي» المتمثّلة في حماية الاتّصالات الأميركيّة من تجسّس الآخرين. باتت «وكالة الأمن القومي» أشد تركيزاً على الشؤون الدفاعيّة، وأكثر انفتاحاً. لكن أعمال التنصّت اكتسبت حياة جديدة أشد كثافة، عقب هجمات الإرهاب في 9/ 11. «لن تتكرّر أبداً». مثّل ذلك الشعار التزاماً مستحيلاً بالطبع[5]، لكن الطريق الوحيد لمنع أي شيء من الحدوث

هـو معرفـة كل ما يحصـل. وأدى ذلـك بـ «وكالة الأمـن القومي» إلى وضـع الكرة الأرضيّة تحت الرقابة.

في أعمال الجاسوسـيّة التقليدية، تتواجه الحكومات مع بعضها بعضاً. ونتجسّس على الحكومات الأجنبيّة والأشـخاص الذين يكونون عمـلاء لها. لكن، كان العدو مختلفـاً في حال الإرهاب. لم يعد الأمر يتعلّق بحفنة من قادة الحكومات «هناك»؛ بل صـار خلايا إرهاب عشـوائيّة من المحتمل أن يكون أعضاؤهـا في أي مكان. ترصد الرقابة الحكوميّة الحديثة كل شخص، يستوي في ذلك المحلي والدولي[6].

وليس ذلك للقول إن رقابة الحكومة للشعب هو أمر جديد. إذ فعلته الحكومات التوتاليتاريّـة طيلـة عقـود في الاتّحـاد السـوفياتي، وألمانيـا الشرقيّـة، والأرجنتـين، والصـين، وكوبا، وكوريا الشـماليّة وغيرها. في الولايات المتّحدة، تجسّسـت «وكالة الأمن القومي» والـ «إف بي آي» على أميركيّين من الأنواع كلها. في سـتينيات القرن العشرين وسـبعينياته، تجسّسـت الوكالة على نشـطاء معارضة الحـرب، قادة الحركة المدنيّة، وأعضاء مجموعات سياسيّة سلميّة متمرّدة. في العقد الأخير، أعادت التركيز مجدّداً على نشطاء مناهضة الحرب وأعضاء مجموعات سياسيّة سلميّة متمرّدة، إضافة إلى المسـلمين الأميركيّـين. وتصاعدت أهمية تلك المهمة الأخـيرة[7]، بعدما صارت «وكالـة الأمـن القومي» الوكالة الرئيسـة المسـؤولة عـن ملاحقـة «القاعدة» خلف البحار.

ترافـق ذلـك التغيـير في الهـدف مـع تطـوّر في تكنولوجيـا الاتّصـالات. قبـل زمـن الإنترنـت، كان مـن السـهل التركيـز عـلى الاتّصـالات الأجنبيّـة. في شـبكة الاتّصالات العسـكريّة الصينيّة، لم يكن هناك سـوى الاتّصالات الصينيّة. استُخدِم نظـام الاتّصـالات الروسي مـن أجل الاتّصـالات الروسـيّة وحدهـا. إذا اخترقت «وكالـة الأمـن القومي»[8] أحـد الكوابـل البحريّة بـين مدينتي «بتروبافلوفسـك»

و«فلاديفستوك» الروسيّين، لم يكن عليها أن تقلق بشأن احتمال أنها اخترقت الاتّصالات بين مدينتي «ديترويت» و«كليفلاند» الأميركيتين.

تعمل الإنترنت بطريقة مغايرة كليّاً. إذ تختلط اتّصالات الناس كلها على الشبكات نفسها. يستخدم الإرهابيّون مقدّمي خدمات البريد الإلكتروني، كالآخرين كلهم. وتحمل الدوائر الإلكترونيّة نفسها اتّصالات الحكومات الروسيّة والإيرانيّة والكوبيّة، متمازجة مع تغريداتك على موقع «تويتر».

وربما تنتهي المكالمات الشبكيّة بين نيويورك و«لوس أنجلوس» إلى كوابل بحرية روسيّة. من المحتمل أن تحوّل المكالمات بين «ريو دي جينيرو» و«لشبونة»، عبر فلوريدا. لا يخزّن «غوغل» بياناتك في مقرّه في «ماونتن فيو»[9]، بل ينشرها في عدد من مراكز تجميع المعلومات عبر العالم: في تشيلي وفنلندا وتايوان والولايات المتّحدة وغيرها. مع تطوّر شبكات الاتّصالات الإلكترونيّة العالميّة، صار من الصعب عدم جمع المعلومات عن الأميركيّين، حتى لو لم يكونوا هم الأهداف المطلوبة.

في الوقت نفسه، شرع الجميع في استعمال البرامج والأجهزة نفسها. سابقاً، كانت الأجهزة الإلكترونية والراديو والكومبيوتر في روسيا تعمل بتقنيّات روسيّة. لم يعد ذلك موجوداً؛ إذ نستخدم جميعنا نظام «ويندوز- مايكروسوفت»، والمحوّلات الشبكيّة لشركة «سيسكو»، ومنتجات الأمن الإلكتروني نفسها. تستطيع شراء هاتف «آي فون» في معظم البلدان. يعني ذلك أن الإمكانات التقنيّة لاختراق الشبكات العسكريّة الصينيّة أو نُظُم المكالمات الهاتفيّة الفنزويليّة مثلاً، قابلة للتعميم عالميّاً.

تحوز الولايات المتّحدة أوسع شبكة للرقابة في العالم بفضل ثلاث ميزات. تملك الميزانيّة الأضخم للاستخبارات[10]؛ إذ تفوق مجموع نظيراتها في الدول كلها. وتؤدّي طبيعة تمديدات شبكة الإنترنت فعليّاً إلى مرور معظم الاتّصالات العالميّة بحدود الولايات المتّحدة[11]، حتى لو كانت بين بلدين مختلفين. وتضم أراضي

الولايـات المتّحـدة معظم الشركات الكـبرى للإنترنت، وتلك التـي تصنع البرامج والأجهزة الأكثر شـعبية وانتشـاراً؛ وهي بالتالي تسـير تحت القوانين الأميركيّة. إنّها المهيمن في ذلك المضمار.

وبجـلاء، يتلخّص هـدف رقابة «وكالة الأمـن القومي»[12]، وفق الاقتباسـات التـي تظهـر في شرائح العـروض الضوئيّـة فائقة السريّـة على موقعها الشـبكي، في: «اجمع كل شيء»، و«اعرف كل شيء»، و«استفد من كل شيء». تخترق «وكالة الأمن القومـي» الإنترنت لدى شركات الاتّصـالات للهواتف والكوابل، كما تجمع البريد الإلكتروني، والرسـائل النصيّة، وتاريخ عمليات البحث بواسطة الإنترنت، ودفاتر العناوين، و«المعلومات المكانيّة»، وكل شيء آخر تستطيع وضع يدها عليه.

لا يوجـد دليـل عـلى أن «وكالة الأمـن القومي» تجمـع المكالمات الهاتفيّـة كلها في الولايات المتّحدة[13]، لكننا نعلم أنها تفعل ذلك في أفغانستان وبرمودا (على الأقل)[14]، تحـت مظلة برنامج «سـومالغِت» (SOMALGET). بلغت ميزانية الوكالة قرابة 10.8 بليـون دولار في 2013[15]، وتوظـف مباشرة قرابة 33 ألف شـخص[16]، إضافة إلى أعداد أخرى ممن يعملون معها بوصفهم متعاقدين[17]. كانت إحدى وثائق سـنودن هي «الميزانيّة السـوداء» الفائقة السريّة، لـ «وكالة الأمن القومي» ووكالات استخباراتيّة أميركيّة أخرى: إذ بلغ مجموعها 53 بليون دولار في 2013[18]. ويقدّر أن الولايات المتّحدة تنفق 72 بليون دولار سنوياً على الاستخبارات[19].

جـاء الكثير من أموال «وكالة الأمن القومي» المخصصـة لبنيتها التحتيّة الرقابية الحديثة من الجهود الحربيّة في أفغانسـتان والعـراق بعد أحداث 9/ 11. كانت تلك جهـوداً هجوميّـة للتعرّف إلى الأهـداف المعادية وتحديد أمكنتها، مـع جهود دفاعيّة للتعـرّف إلى أدوات التفجـير البدائيّـة والعمل على تفكيكها. يعنـي ذلك أن قدرات الوكالـة تطوّرت بمواجهة شـبكات في تلك البلدان[20]؛ وكذلك لأن كل شـخص

على الكرة الأرضيّة يستخدم المعدّات نفسها، صار ممكناً استعمال تلك المعدات ضدّ النُظُم في أمكنة مختلفة.

ثمة سؤال يبرز بشكل واضح: هل ذلك العمل قانوني؟ الجواب الحقيقي هو أننا لا نعلم، إذ تأتي السلطة الحالية لـ «وكالة الأمن القومي» من ثلاثة أمكنة:

الأمر التنفيذي رقم 12333 [21]، موقّعاً من الرئيس رونالد ريغان في 1981، ويجيز للوكالة إجراء رقابة واسعة في الخارج. ويتضمّن بعض الحماية للمواطنين الأميركيّين وحدهم[22]، لكنه يجيز عمليات واسعة في جمع المعلومات عن الأميركيّين وتحليلها والاحتفاظ بها.

الفصل 215 من التشريع الأميركي «قانون باتريوت» (Patriot Act[23] USA)(*) الذي سنّ عام 2001، ويسمح للوكالة بأن تجمع «أي شيء ملموس (بما فيها الكتب والتسجيلات والأوراق والوثائق والمكوّنات الأخرى)»- عن كل شخص، وليس الأجانب وحدهم- «خدمة لتحقيق هدفه في الحماية من الإرهاب الدولي والنشاطات الاستخباراتيّة السريّة». ربما بدت الكلمات الأخيرة كأنها تقييد، لكن محكمة سريّة فسّرتها[24] بطريقة تجعلها تشمل الجمع المستمر لـ «البيانات الوصفيّة» عن المكالمات الهاتفيّة لكل أميركي.

الفصل 702 من تعديلات قانون «فيسا» (FISA) [25]، اختصاراً لعبارة «قانون رقابة الاستخبارات الأجنبيّة» (Foreign Intelligence Surveillance Act) للعام 2008، وأجاز للوكالة بمفعول رجعي نشاطات لتجميع المعلومات كانت أجرتها بطريقة غير قانونيّة بعد 9/ 11. كما وسّع نطاق اختصاص الوكالة بما يسمح لها بجمع المعلومات عن الأجانب، مع وجود حماية ضئيلة تماماً للمواطنين الأميركيّين. استخدمت الوكالة تلك السلطة لترصد الهيكل العام لبنية اتّصالات الإنترنت أثناء دخولها أميركا، مع حصد البيانات عن الأجانب والأميركيّين معاً.

(*) الترجمة الحرفيّة للكلمات هي "شرعة الأميركي الوطني"

هناك سبب مزدوج لعدم وضع حدّ للنقاش عند هذه النقطة. أولاً، لا يتمتع عدد من تدابير الرقابة التي تضمّنتها تلك القوانين بالدستوريّة الكافية؛ سواء ما يتعلّق بالتفتيشات أم المصادرات غير الشرعيّة. وثانياً، بعض تفسيرات «وكالة الأمن القومي» لتلك القوانين هي بالتأكيد غير شرعيّة، وتناقش المحاكم حالياً تحدّيات رفعت في وجهه تلك المسالك. أعتقد أنه في النهاية، سوف توقف المحاكم كثيراً مما تفعله الوكالة حاضراً، وكذلك سوف توقف تشريعات جديدة مقبلة كمية أكبر من تلك الأفعال. بالطبع، حينها سيكون الأميركيّون قد عانوا عقوداً من الرقابة الواسعة، وهو ما يحتمل أنه استراتيجيّة الوكالة أصلاً. سوف أناقش ذلك بمزيد من التوسّع في الفصل 13.

تجمع «وكالة الأمن القومي» معلومات كثيرة عن الأميركيّين، بعضها يبدو «عرضيّاً». بقول آخر، إذا راقبت الوكالة شبكة هواتف في فرنسا، فلسوف تجمع معلومات عن مكالمات بين الولايات المتّحدة وفرنسا. وإذا ترصّدت كابل بحري للإنترنت في مياه المحيط الأطلسي، فلسوف تحصد معلومات عن أميركيّين يصادف أن الحركة الإلكترونيّة المتّصلة بنشاطاتهم جرى تحويلها بذلك الكابل. وهناك قوانين تقليصيّة للوكالة[26]، هدفها الحدّ من قدرتها على جمع معلومات عن الأميركيّين وتحليلها وتخزينها، على الرغم من أن معظم ما علمناه عن تلك القوانين يشير إلى أنها ليست فعّالة عمليّاً. هنالك قوانين مختلفة عن محتوى الاتّصالات من جهة، و«البيانات الوصفيّة» من ناحية ثانية؛ ويعتمد الفارق في القوانين على السلطة الشرعيّة التي تستند إليها الوكالة في تبرير اختراقاتها. ولا يعني التقليص الوصول إلى حدّ حذف المعلومات عن الأميركيّين، بل مجرد حفظ المعلومات مع إغفال الهويّات؛ بانتظار أن يأتي أحد ما ويطلب أن يرى ما هي عليه فعليّاً. تمارس الوكالة كثيراً من المخادعة مع القوانين في ذلك المضمار[27]، وحتى أولئك الذين يحاولون التدقيق في نشاط الوكالة يقرّون بأنهم لا يستطيعون تخيّل ما تفعله الوكالة حقاً.

في 2014، ظهـر تحليـل عن وثائق قدّمها سـنودن[28]، بشـأن بعض ما حصلت عليـه الوكالة فعلياً في سـياق اختراقها الحركة الإلكترونيّة عـلى الإنترنت. وتبيّن أن بيانات عن أشـخاص أبرياء، أميركيّين وغير أميركيّـين، فاقت تلك التي جُمِعَت عن أهـداف جـرى تشريع رقابة الاسـتخبارات عليها. يعبّر الأمر عـن بعض من طبيعة عمل الاسـتخبارات. وحتى المعلومات المقلّصة عن شـخص ما سـوف تحتوي على اتّصالات مع أشخاص أبرياء؛ لأن كل اتّصال- حرفيّاً- مع هدف ما، يقدّم أي نوع من المعلومات المثيرة للاهتمام؛ سيجري الاحتفاظ به.

ربما تتصدّر «وكالة الأمن القومي» صفحات الجرائد، لكن مجتمع الاستخبارات الأميركيّـة يضـمّ فعليّـاً 17 وكالـة مختلفـة. بالطبع، هنالـك «وكالة الاسـتخبارات المركزيّـة» («سي آي إيـه»). ربـما سـمعت عـن «نـرو» (NRO)، الاسـم المختـصر لـ«المكتـب الوطنـي للاسـتطلاع» (National Reconnaissance Office)، ويتـولى مسـؤولية الأقـمار الاصطناعيّة للبلاد. وهناك وكالة اسـتخبارات لـكل من الفروع الأربعة للجيش. وتمارس الرقابة «وزارة العدل» (كلاًّ من الـ«إف بي آي» و«مكتب مكافحة المخدرات»)، والدولة، والطاقة، والخزانة، و«الأمن الوطني» (Homeland Security)، إضافة إلى بضع وكالات أخرى. ربما يكون هناك الوكالة الـ18 السريّة. (ليـس أمراً مرجّحـاً، لكنه محتمل. إذ بقيـت تفاصيل مهمة «وكالـة الأمن القومي» سريّة حتى سبعينيات القرن الماضي، بعد عشرين سنة من إنشائها).

بعد «وكالة الأمن القومي»، تبدو الـ«إف بي آي» الوكالة الحكوميّة الأكثر غزارة في ممارسة الرقابة. وتربطها علاقات وثيقة مع «وكالة الأمن القومي»[29]، ويتقاسم الطرفان المعلومات والتقنيّات والسـلطات التشريعيّة. من السـهل نسيان أن الوثيقة الأولى لسنودن نشرتها صحيفة الـغارديان البريطانيّة- وكانت كناية عن الأمر الذي صـدر لشركة «فريزون» لتسـليم «البيانـات الوصفيّة» عن زبائنهـا كلّهم- تضمّنت أيضـاً أمـراً للـ «إف بي آي» بتسـليم المعلومات إلى «وكالة الأمـن القومي». ونعرف أنـه يوجد تشـارك كثيـف[30] في المعلومات بـين «وكالة الأمن القومـي» و«سي آي

إيـه» و«وكالـة مكافحة المخـدرات» و«وكالة الاسـتخبارات العسـكريّة» و«وزارة الأمن الوطني». ويعمل أحد برامج «وكالة الأمن القومي» الذي يحمل اسـماً مشفّراً هـو «أي سي ريتـش» (ICREACH)، على إمداد 23 وكالـة حكوميّة بمعلومات عن أميركيّين.

وإذ قيـل ذلك، وعلى عكس «وكالة الأمن القومي»، تتميّز الرقابة التي تمارسـها الـ«إف بي آي» بأنها تخضع تقليديّاً لمراجعة من السـلطة التشريعيّة، بواسـطة عملية الحصول على مذكّرات تفتيش قانونيّة. ووفق التعديل الرابع في الدستور الأميركي، يجـب على الحكومـة أن تبرهن لقاضٍ أن عملية التفتيش يمكن أن تكشـف أدلة عن جريمـة، بطريقـة معقولة. في المقابل، تملك الـ«إف بي آي» سـلطة أن تتولى جمع، من دون مذكـرة قانونيّـة، معلومات شـخصيّة من الأنـواع كلها؛ سـواء بطريقة موجهة لأفراد أم باسـتهداف مجموعات كبيرة باسـتخدامها «رسـائل الأمـن القومي» التي تتمثّل أساساً في مذكّرات توقيف تصدرها الـ«إف بي آي» من دون مراجعة قضائيّة. وجرى توسـيع أمديـة تلك المذكّرات في 2001، بقانـون «باتريوت آكت» (الفصل 55 منـه)، عـلى الرغم من أن الأسـس القانونيّـة الأصلية لتلك الرسـائل ترجع إلى العام 1978[31]. وحاضراً، تسـتعمل الرسـائل عمومـاً في الحصول على معلومات مـن طرف ثالث: رسـائل البريد الإلكـتروني في «غوغل»، والسـجلات البنكيّة من المؤسّسات الماليّة، وملفّات من موقع «دروب بوكس» (Dropbox).

في الولايـات المتّحـدة، عمدنا إلى تخفيض حقوق الخصوصيّـة على تلك البيانات كلها، بسـبب ما يسـمّى بـ«مبدأ الطـرف الثالث». ففي العـام 1976، سرق مايكل لي سـميث امـرأة في «بالتيمـور»، ثـم دأب على مضايقتهـا بالهاتـف. وبعدما عثرت الشرطـة على شـخص تتشـابه أوصافه مع سـميث، طلـب من شركة الهاتف إنشـاء «سـجل مكتوب» عن الخط الهاتفي لسـميث، مع تسـجيل كل أرقـام الهواتف التي يتصـل بها. بعـد التأكّد من أنّ سـميث اتّصل بالمـرأة، حصلت الشرطـة على مذكرة تفتيش لمنزله، واعتُقِل سـميث بتهمة السرقة. حاول سـميث إبطال الأهمية القانونيّة

لـ«السـجل المكتوب» لأن الشرطة لم تحصل على تفويض قانوني بإنشائه. في 1979، قـرّرت «المحكمـة العليـا» أنـه لم يكن من الـضروري الحصول عـلى تفويض قانوني لإنشـاء «السـجل المكتوب» عن مكالمات سـميث الهاتفيّة، قائلة: «إنّ هذه المحكمة رأت باسـتمرار أن المرء لا حق له بتوقّعات قانونيّة، بشأن معلومات سلّمها طواعيّة إلى طرف ثالث». وتعني تلك الكلمات أساسـاً، أنه بسـبب مشـاركة سـميث أرقام الهواتـف التي يتحدث إليهـا مع شركة الهاتف[32]، فإنّه يفقد الحقّ في توقّع أن تحظى تلـك المعلومـات بأي نوع من الخصوصيّـة. ربما بدا ذلك منطقيّـاً في 1979، عندما كانت معظم معلوماتنا وبياناتنا تحت سـيطرتنا، وقريبـة منا. ولكن حاضراً، تتجمّع معلوماتنا كلها في «سحابة» لا نعرف مكانها، ويمسك بها مجموعة من أطراف ثلاثة، وهي متفاوتة في درجة الموثوقيّة.

عـزّزت التقنيّة كثيراً قدرة الـ «إف بي آي» على ممارسـة الرقابة من دون الحصول على تفويض قانوني. ومثلاً، تستخدم الـ «إف بي آي» (وكذلك الشرطة المحلية)، أداة إلكترونيّة تسـمّى «آي أم أس آي- كاتشر» (IMSI– Catcher)[33] التي هي أساسـاً برج لاتّصالات الخلوي، لكنه زائف. إذا كنت سمعت عن ذلك، فلا بد أنك سمعت عن اسـم شيفري هو «ستنغراي» (StingRay)[34]، وهو عمليّاً نوع من «آي أم أس آي- كاتشر» تبيعه شركة «هاريس كوربوريشـن». وعند تفعيل ذلك البرج، تنخدع به الهواتف الخلوية القريبة منه، فتتصل به. وبمجرد حصول ذلك، يعمل «آي أم أس آي- كاتـشر» على جمـع بيانات عن أمكنة تلك الهواتف وهويّاتهـا[35]، بل إنه أحياناً يسـتطيع التنصّت على المكالمات الصوتيّة، والرسائل النصيّة، وعمليات الدخول إلى الإنترنت بواسـطة الخلوي. ويسـتحوذ الذعر على الـ «إف بي آي» بشـأن شرح تلك القـدرة للجمهـور[36]، إلى حدّ أنّها تفرض على الشرطـة المحلية توقيع اتفاقيّات عن عدم الكشـف عنها، قبل اسـتخدام تلك التقنية؛ وتوجّه الشرطة بأنها تكذب بشـأن اسـتعمال «آي أم أس آي- كاتشر» في المحاكم[37]. وعندما بدا أن الشرطة المحلية في مدينة «ساراسوتا» بولاية فلوريدا قد تكشف وثائق معدّات «ستنغراي» القادرة على

اعتراض المكالمات الخلوية المحليّة إلى المدعين في قضية حقوق مدنيّة رفعت ضدهم، صادر الضباط الفدراليّون تلك الوثائق[38].

يصعب الإحاطة تماماً بالمنظمات الحكومية الأميركية المنخرطة في الرقابة. يحتفظ «المركز القومي لمكافحة الإرهاب»[39] بسجل عن «بيئة البيانات المتّصلة بهويات الإرهاب كافة»، وهي مؤسّسة تشكّل مخزناً لمعلومات الحكومة عن الإرهابيّين الدوليّين المشتبه فيهم. وفي 2007، كانت المؤسّسة تحتفظ بقاعدة بيانات ضخمة عن المواطنين الأميركيين[40]، وتُبقي عينها مفتوحة على قرابة 700 ألف مُعَرّف (ما يشبه كونهم أشخاصاً، لكن ليس بالضرورة)، وهي مصدر قوائم الرقابة المختلفة[41]. وتبدو عمليّات التعامل مع تلك القوائم اعتباطيّة[42]، وعندما يجري التركيز على أحدهم يصبح كمن لا ملاذ آمن له. كان اسم تامرلان تسارناييف، المفجّر في «ماراثون بوسطن»، على إحدى تلك القوائم[43].

هناك أيضاً «فرق العمل لدعم مكافحة الجريمة المنظّمة»[44] الذي يعمل مع التحقيقات المتعلّقة بالمخدّرات، و«المبادرة الوطنية الشاملة لأمن الفضاء السبراني»[45](*)، وهي تتعامل مع التهديدات التي تطال الحواسيب. ويعمل «مكتب الكحول والتبغ والأسلحة الناريّة» على بناء قاعدة معلومات ضخمة بهدف تتبع الناس وأصدقائهم[46]. وحتى البنتاغون مارس التجسّس على الأميركيّين[47]، بواسطة وكالة لا تحظى بشهرة واسعة اسمها «النشاط لمكافحة التجسّس على الأرض» التي أُغلِقَت في 2008. في 2010، راقب «مكتب القوات البحريّة للتحقيق الإجرامي»[48] كل كومبيوتر في ولاية واشنطن يحتوي برنامجاً للتشارك في الملفات بين الجمهور، سواء أكان مرتبطاً بالجيش أم لا، ما مثّل تعدياً واضحاً على القانون.

(*) نفضل استخدام تعبير «السبراني» ترجمة حرفية لـ(Cyber)، رغم إدراكنا ثقلها وعدم شيوعها؛ تمييزاً لها عن تعبير الإلكتروني أو الافتراضي أو الشبكي، التي تتقاطع معها أحياناً من حيث المعنى.

تجري مجموعة كبيرة من نشاطات الرقابة على البيانات والمعلومات، خارج أطر الحكومة الفيدراليّة الأميركيّة. فمنذ 9/ 11، أنشأت الولايات المتّحدة «مراكز انصهار» ونشرتها في أرجاء البلاد[49]. وبوجه عام، تدار تلك المراكز من قِبَل السلطات المحليّة في كل ولاية، بالتعاون مع قوى الشرطة فيها. وقُصِد من المراكز أن تكون جسراً للمعلومات بين تلك السلطات المحليّة والوكالات القوميّة كالـ «إف بي آي» و«وزارة الأمن القومي». وتمنح المراكز للشرطة المحلية حق وصول لم يكن متاحاً لها من قبل[50] إلى بيانات الرقابة وقدراتها، وافتُرِضَ أساساً أنها سوف تركّز على الإرهاب[51]، لكنها استعملت لدعم إنفاذ القانون على نطاق يتوسّع باطّراد. ولأنّها تدار محليّاً، تتفاوت القوانين التي تتّبعها بين مركز وآخر، كما يتفاوت مستوى الالتزام بالقوانين أيضاً. هنالك قليلٌ من الإشراف القانوني[52]، وربما بعض التدخل غير القانوني من الجيش، وكثيرٌ من السريّة. ومثلاً، يعرف عن تلك «مراكز الانصهار» أنها راقبت محتجّين سياسيّين[53].

تدار «الفرق المشتركة لمكافحة الإرهاب» محليّاً أيضاً، وهي معرّفة بطريقة ضبابيّة، ومحاطة بسريّة فائقة[54]. وتورّطت في التحقيق مع نشطاء سياسيّين[55]، ونشر الدعاية المضادة للإسلام[56]، ومضايقة مدنيّين أبرياء[57].

وبصورة إجماليّة، ثمة سيل كبير من الرقابة يمارس في الولايات المتّحدة، تقوده ميول إيديولوجيّة، وتلابسه حماسة مفرطة.

وفي الطرف الآخر من المحيط الأطلسي، تمثّل «القيادة الحكوميّة للاتّصالات» النظير البريطاني لـ «وكالة الأمن القومي». وتنخرط في عمليات تجسّس واسعة على مواطنيها وعبر العالم أيضاً، انطلاقاً من مقرّاتها في بريطانيا، ومراكز تنصّت في عُمان[58] وقبرص[59] وغيرهما. وتشكّل شريكاً مقرّباً من «وكالة الأمن القومي»، وتمارس رقابة عامة داخل حدود بلادها وخارجها. وتشمل قائمة البلدان التي تتنصّت على مواطنيها ومواطني دول أخرى: ألمانيا[60]، فرنسا[61]، الدانمارك[62]،

أستراليا[63]، نيوزيلندا[64]، إسرائيل، كندا... وربما كل دولة تملك مالاً كافياً كي تخصّصه لأعمال الاستخبارات[65]. وتزعم الحكومة الأستراليّة أن رقابتها في أندونيسيا ساعدت في إجهاض هجمات إرهابيّة في ذلك البلد[66].

نعرف قليلاً جداً عن الرقابة الحكوميّة في بلدان أخرى، لكننا لا نفترض أن أموراً مشابهة لا تحدث هناك، لمجرد عدم وجود من يدق النفير ويلقي ضوءاً كاشفاً عليها. تنهض الحكومات الأخرى بأشياء مماثلة حيال الإنترنت، ووفق ما تستطيع أن تضع يدها عليه، مع وجود قيود قانونيّة أقل على نشاطات تلك الحكومات في الرقابة.

إذ إن روسيا تجمع وتخزّن وتحلّل البيانات عن المكالمات الهاتفيّة[67]، الـ «إيميل»، استخدام الإنترنت، شبكات التواصل الاجتماعي، معاملات البطاقات الائتمانيّة وغيرها. وأنشأت «نظام التحقيقات والإجراءات العملانية»، ويعرف باسمه المختصر «سورم» (SORM)، استناداً إلى البنية الروسيّة على الإنترنت[68]. ورأينا لمحات عن المدى الواسع لعمل «سورم» أثناء دورة الألعاب الشتويّة في «سوتشي» 2014[69]. وحينها، تمكّنت السلطات الروسيّة من رقابة معظم ما يجري على خطوط الإنترنت في بلدها. أعطى الإرهاب والجريمة ذرائع للرقابة، لكنها تصل إلى معلومات تستعمل ضد الروس من صحافيين ونشطاء حقوق الإنسان ومعارضين سياسيّين[70].

تحاول الصين أيضاً ترصّد كل أفعال مواطنيها على الإنترنت[71]، وبدرجة أكبر خارج تلك الشبكة أيضاً. وتستخدم الصين أيضاً «المعلومات المكانيّة» من الهواتف الخلوية كي تتعقّب الناس جماعيّاً[72]. وتخترق الخلويات عن بُعد كي تتنصّت على الناس[73]، كما تراقب الأمكنة العامة بواسطة ما يتراوح بين 20 مليون و30 مليون كاميرا للرقابة[74]. وعلى غرار روسيا، تشكّل الجريمة التبرير المعلن لذلك التجسّس كله، لكن الانشقاق يمثّل حجّة كبرى أيضاً. ويمثّل «توم- سكايب» (TOM- Skype) نظاماً لخدمات التراسل بالفيديو والرسائل النصيّة، وهو مبادرة

مشـتركة بين «مايكروسـوفت» وشركة «توم أون لاين» الصينيّة. إنّ الرسـائل التي تحتـوي كلـمات[75]، كـ «تيانانمـن» و«منظّمـة العفـو الدوليّـة» و«هيومـن رايتـس ووتـش» (Human Rights Watch) [«المنظّمـة الدوليّة لحقوق الإنسـان»]، وكذلك الإشـارات إلى المخدّرات والأفلام الإباحية الجنسـيّة، تنسخ وتخزّن كلها. ويعمل ما يزيد على 30 ألف رجل شرطة في رقابة الإنترنت[76].

قبـل بضع سـنوات، مرّت أمام أعيننـا لمحات من الرقابـة العالميّة على الإنترنت، عندمـا هـدّدت الهنـد[77]، وروسـيا[78]، والسـعودية[79]، وأندونيسـيا[80]، ودولة الإمـارات العربيّـة المتّحـدة[81]، بحظـر شركـة «بـلاك بـيري» (Black Berry) ما لم تسمح لتلك الدول بالدخول إلى البيانات عن اتّصالات المستخدمين. عقدت «بلاك بيري» اتفاقيّة مع الهند[82]، احتفظت الشركة بموجبه بأمن بيانات مسـتخدمي تلك الهواتـف، مقابل حق الحكومـة في الوصول في حالات فرديّـة إلى البريد الإلكتروني للمسـتخدمين، ومحادثاتهـم الإلكترونيّة، والمواقع التـي يدخلونها على الإنترنت. لا نعـرف ما هي الصفقات التي أبرمت مع بقية الدول، لكن من المسـتطاع أن نفترض أنها سارت على نحو مماثل.

وغالبـاً، تلجأ الدول الصغيرة إلى الكبيرة للحصول على مسـاعدتها في بناء بنيتها التحتيّـة للرقابـة. حصلت إيران على مسـاعدة الصـين في بناء رقابة مندمجـة مع بنية الإنترنت فيها[83]. وسأستفيض في الفصل 6 في الحديث عن الشركات الغربية التي تساعد حكومات قمعيّة في بناء نُظُم للرقابة.

إنّ الأفعـال التـي تأتيهـا تلـك البلـدان وغيرهـا- أسـتطيع وضع كتـاب مملوء بالأمثلة عنها- لهي أشد قمعاً وتوتاليتاريّةً من الولايات المتّحدة وحلفائها كافة[84]. وتفـرض الولايـات المتّحدة تحديدات وقيـوداً قانونيّة على عمليـات جمع المعلومات مـن قِبَل الحكومة[85]، مـا يفوق بكثير الدول الأخرى على الكـرة الأرضيّة، بما فيها الاتحّـاد الأوروبي. في الهنـد[86] وتايلاند[87] وماليزيا[88]، يمثّـل اعتقال الناس بأثر

من محادثات شبكية ونشاطات على الإنترنت عُرفاً سائداً. سأتحدث عن المخاطر والأضرار في الفصل 7، أما الآن، فسوف أقصُر حديثي على القدرات.

الحكومة بوصفها «هاكر»

هناك فارق هائل بين التجسّس الإلكتروني كما كانه إبّان «الحرب الباردة»، وحاله حاضراً. قبل عصر الإنترنت، عندما كانت الرقابة تتكوّن أساساً من تجسّس الحكومات على بعضها بعضاً، يجب على مؤسّسات كـ «وكالة الأمن القومي» أن تستهدف دارات إلكترونيّة محدّدة، كأن تكون كابلاً بحرياً للاتّصالات يربط بين مدينتي «بتروبافلوفسك» و«فلاديفستوك»، قمراً اصطناعياً للاتّصالات، وشبكة لربط الهواتف بنظام الموجات الفائقة الصغر («ميكروويف»). وفي معظم الأحيان، كان ذلك النشاط سلبيّاً ولا يستلزم سوى زرع رادارات كبيرة في دول مجاورة.

في المقابل، تعتمد الرقابة الحديثة على الانخراط بفعاليّة في اختراق شبكات الكومبيوتر عند العدو، وزرع برامج خبيثة مصمّمة كي تسيطر على تلك الشبكات و«ترشيح الملفات إلى خارجها»، وفق تعبير تستخدمه «وكالة الأمن القومي» لوصف سطوها على الملفات. وبقول أشد صراحة، لم تعد الطريقة الأسهل للتجسّس على اتّصالاتك هي اعتراضها أثناء نقلها بالشبكات، بل اختراق كومبيوترك والدخول إليه.

وتجري الحكومات مجموعات ضخمة من عمليات اختراق الحواسيب.

في 2011، استطاع «هاكر» إيراني أن يخترق نظام الكومبيوتر في سلطة المصادقة الإلكترونيّة في الدانمارك[89]، واسمها «ديجينوتار» (DigiNotar). وبفضل ذلك، استطاع ذلك الـ«هاكر» أن ينتحل هويّة كيانات إلكترونيّة كبرى تدخل إلى الإنترنت في الدانمارك بعد حصولها على مصادقة من «ديجينوتار». وبذا، انتحل هويّة مؤسّسات كـ«غوغل» و«سي آي إيه» و«أم آي 6» و«موساد» و«مايكروسوفت» و«ياهوو»

و«سكايب» و«فيسبوك» و«تويتر» و«خدمة تحديث نظام ويندوز» وغيرها. وبذا، بات متاحاً له أن يتجسّس على مستخدمي تلك الخدمات. وكذلك درّب آخرين على تلك القدرة[90]- تحت إشراف شبه مؤكّد من الحكومة الإيرانيّة- الذين استعملوا تلك الطريقة في الرقابة الجماعيّة لإيرانيّين، بل ربما لأجانب أيضاً. وحينها، قدّرت شركة «فوكس- آي تي» (Fox- IT) أنّه جرى اختراق 300 ألف حساب إيراني على بريد «جي ميل» الإلكتروني[91].

في 2009، عثر بحّاثة كنديون على جزء من برنامج خبيث اسمه «غوست نت» (GhostNet) [92]، في كومبيوترات الدالاي لاما، المعارض للحكومة الصينيّة. ومثّل «غوست نت» برنامجاً متطوّراً لشبكة رقابة يديرها كومبيوتر في الصين. ومع التعمّق في البحث، عُثِر على ذلك البرنامج عينه في كومبيوترات مؤسّسات سياسيّة واقتصاديّة وإعلاميّة، موجودة في 103 بلدان. باختصار، كانت تلك قائمة الأهداف الأكثر تفضيلاً لدى الاستخبارات الصينيّة. ويمثّل برنامج «فلايم» (Flame) أداة للرقابة الإلكترونيّة[93]، وعثر عليه الباحثون في الشبكات الإيرانيّة في 2012؛ ونعتقد بأنّ إسرائيل والولايات المتّحدة زرعتاه هناك وفي أمكنة أخرى. واستمر برنامج «ريد أكتوبر» (RedOctober) [94] في التجسّس بخفاء على الكومبيوترات في العالم، إلى أن عُثِر عليه في العام 2013، ويعتقد بأنّه يمثّل نظاماً روسيّاً للرقابة. ويشبهه فيروس «تورلا» (Turla) الذي تجسّس على حكومات غربيّة، واكتُشِف في 2014 [95]. وفي العام 2014 أيضاً، اكتُشِفَ فيروس «ماسك» (Mask) [96] الذي يعتقد بأنه إسباني، وهو برنامج للرقابة. واستهدف «هاكرز» إيرانيّون حواسيب مسؤولين رسميّين أميركيّين[97]. هنالك أكثر من ذلك بكثير من الأدوات المعروفة للرقابة الإلكترونيّة، ويسود اعتقاد بأن أعداداً أخرى سوف يجري اكتشافها مستقبلاً.

من باب الإنصاف، يجب القول إنّنا لا نملك أدلّة تربط برامج الرقابة ببلدان بعينها، ولا حتى بوجود إشراف حكومي عليها. ففي معظم الأحيان، تمتنع الحكومات عن الاعتراف بأنها تخترق نظم الكومبيوتر لدى بعضها بعضاً. ومثلاً، ضمّت قائمة

الأهـداف في برنامـج «ماسـك» معظم البلـدان المتحدّثـة بالإسـبانيّة، ومجموعة من الكومبيوترات في المغرب وجبل طارق. ويبدو ذلك كأنّه من فعل إسبانيا.

في الولايات المتّحدة، كانت المجموعة التي أدينت باختراق نُظُم الكومبيوتر هي «مجموعـة عمليات الدخول المنسّـقة» (Tailored Access Operations group)[98]، واشـتهرت باسـمها المختـصر «تاو» (TAO)، وهـي ضمن «وكالة الأمـن القومي». نعـرف أن مجموعة «تاو» تتسـلل إلى الكومبيوترات عن بُعد[99]، مسـتخدمة برامج تحمـل أسـماء شـيفريّة كـ «كوانتـوم إنـسرت» و«فوكس أسـيد». ونعـرف أن «تاو» طوّرت برامج كومبيوتر مختصّة تستطيع اختراق الأشياء الإلكترونيّة كافة[100]، من الكومبيوتر مروراً بمحوّلات الإنترنت، ووصولاً إلى الهواتف الذكيّة. واسـتطاعت «تاو» أن تحوّل بعض مكوّنات لا سلكيّة في حواسيب كثيرة، إلى «عملاء مزروعين» لها، بواسـطة اعتراض إرسـالها واسـتخدام موجاتها لدس برامج خبيثة فيها. ويشير أحـد التقديـرات إلى أن تلـك المجموعة نجحـت في اختراق 80 ألـف كومبيوتر في العالم، وباتت تحصل على ملفات «ترشح» منها[101].

بديهـي القـول إننـا صرنـا نعـرف عـن «تـاو» والجهـود الأميركيّـة في اخـتراق الكومبيوترات، بعد أن كشـف إدوارد سـنودن وثائق عالية السريّة لـ «وكالة الأمن القومـي». لم تحصـل تسريبات مماثلة في دول أخرى، لذا لا نعرف سـوى القليل عن قدراتها في ذلك المجال.

نعـرف أشـياء كثيرة عـن الصـين[102]. وبموثوقيّة كبـيرة، جـرى تحديد الصين بوصفهـا مصـدراً لهجمات كثـيرة عالية المسـتوى طالـت «غوغـل»[103] والحكومة الكنديّـة[104]، وصحيفـة نيويورك تايمـس[105]، وشركات أميركيّـة[106] من بينها شركـة «آر أس إيـه»(*) (RSA) الأمنيّـة[107]، والمؤسّسـة العسـكريّة الأميركيّة[108]

(*) شركة تصنع تقنية تشفير المفتاح العام في أمن المعلومات، يتكوّن اسمها من الحروف الأولى لمبتكريها، وهم ريفست، وشامير، وآدلمان.

والمتعاقدين معها. في 2013، اكتشف بحّاثة برمجيّات خبيثة للحكومة الصينيّة في عدد من هواتف الـ «آندرويد»[109]، التي يستعملها أفراد من المعارضة المنادية باستقلال إقليم التيبيت عن الصين. في 2014، اخترق «هاكرز» صينيّون[110] قاعدة بيانات «المكتب الأميركي لإدارة الموارد البشريّة» تحتوي على معلومات عن 5 ملايين موظف حكوميّ ومتعاقد يملكون إجازات أمنيّة.

ما سبب تلك الاختراقات؟ يشكّل التجسّس السياسي والعسكري جزءاً كبيراً منها، لكن بعضها تجسّس تجاري. هناك عدد من الدول لديها تاريخ طويل من التجسّس على شركات أجنبيّة لأغراض عسكريّة وتجاريّة[111]. تزعم الولايات المتّحدة أنها لا تمارس التجسّس التجاري، يعني ذلك أنها لا تخترق شبكات الشركات الأجنبيّة وتسطو على معلوماتها، ثم تمرّرها إلى الشركات الأميركيّة المنافسة كي تستفيد منها. لكنها تمارس التجسّس الاقتصادي[112]، باختراقها شبكات الشركات الأجنبيّة وأخذ معلومات منها كي تستخدمها الحكومة في مفاوضات تجاريّة، تستفيد منها مباشرة الشركات الأميركيّة ومصالحها. تأتي أمثلة حديثة على ذلك من شركة «بتروبراس» للنفط في البرازيل[113]، ونظام «سويفت» الأوروبي للمعاملات البنكيّة العالميّة[114]. في الحقيقة، تفاخر تقرير حكومي أميركي صدر في 1996، بادّعاء «وكالة الأمن القومي» أنّ الصناعة الأميركيّة استفادت اقتصاديّاً من أحد برامجها[115]، «بما يصل إلى بلايين الدولارات في سنوات قليلة سابقة». ربما تكون ممن يرون أو أولئك الذين لا يرون فارقاً أساسيّاً بين نوعي التجسّس؛ لكن الصين التي لا يوجد فيها فارق واضح بين أعمال الحكومة والشركات، هي ممن لا يرون فارقاً بين الأمرين.

تشتري بلدان كثيرة برامج من شركات خاصة كي تستخدمها في عمليات اختراق الحواسيب. سأتحدّث بالتفصيل عن ذلك النوع من العلاقة التجاريّة في الفصل 6. وسأتناول الآن إحدى الشركات الإيطاليّة التي تصنع أسلحة للفضاء السبراني، واسمها «هاكينغ تيم» (Hacking Team)[116]، وتبيع نُظُماً للاختراقات

إلى حكومات عدّة كي تستخدمها الأخيرة في اختراق نُظُم التشغيل في الحواسيب والهواتف الذكيّة. ويتسلّل برنامج «هاكينغ تيم» المختص بالهواتف النقّالة إلى دواخل تلك الأجهزة، بعد أن يُرسَل إليها عن بُعد، ثم يتولى جمع البريد الإلكتروني، الرسائل النصيّة، تواريخ المكالمات، دفاتر العناوين، بيانات عمليات البحث على الإنترنت، والضربات الأساسيّة على لوحة المفاتيح. وكذلك يستطيع صنع صور عن شاشة الهواتف، ورصد التراسل بين الخلوي ونظام الـ «جي بي إس». وبسريّة تامة، يرسل البرنامج تلك المعلومات كلها إلى الجهة التي تستخدمه. استخدمت إثيوبيا ذلك البرنامج للتسلل إلى أجهزة صحافيّين أميركيّين وأوروبيّين[117].

لعلّه من المنطقي الافتراض أن معظم الحكومات تمتلك قدرات على الاختراق الإلكتروني. أما مسائل من نوع ضد مَنْ تستخدم تلك القدرات، وما هي القيود القانونيّة للسيطرة عليها، فتلك أمور تتفاوت بين دولة وأخرى.

الهجمات الحكوميّة

عندما تلقينا التقارير الأولى عن اختراق صينيّين للشبكات الأميركيّة بهدف التجسّس، شجبنا ذلك الأمر بلغة قاسية. وصنّفنا الأفعال الصينيّة[118]، كـ «هجمات سبرانية»، وأحياناً رميناها بمصطلح «حرب سبرانيّة»[119]. وبعد أن كشف سنودن أن «وكالة الأمن القومي» كانت تفعل تماماً ما يقوم به الصينيّون، على مستوى العالم بأسره، استخدمت الولايات المتّحدة عبارات ملطفة كثيراً في وصف أفعالها[120]، مستخدمة مصطلحات كـ «تجسّس» و«جمع معلومات» أو «وضع العين»؛ مشدّدة على أنها نشاطات تتعلّق بأزمنة السلم.

عندما حاولت شركة «هواوي» (Huawei) الصينيّة[121] بيع معدّات شبكيّة إلى الولايات المتّحدة، جرى النظر إلى ذلك المسعى باعتباره «تهديداً للأمن القومي» بسبب

الخشـيّة من أن تكون الحكومة الصينيّة قد دسّـت «أبواباً خلفيّة»(*) لتسريب المعلومات من تلك الشبكات إليها. ولاحقاً، عرفنا أن «وكالة الأمن القومي» تفعل الأمر نفسه[122] في معدات شركة «هواوي»، وكذلك المعدّات الأميركيّة التي تُباع في الصين[123].

هناك مشكلة في أنّه من وجهة نظر الضحيّة، يتشابه الهجوم السبراني مع التجسّس الدولي إلى حـدّ كبير[124]. إنّ التجسّـس السـبراني الحديث هو أحد أشـكال الهجوم السـبراني[125]، إذ يتضمّـن كلاهمـا اختراق الشـبكات في بلد آخـر. ويتمثّل الفارق الوحيد بينهما في تعمّد زعزعة الشـبكات المخترَقَة وإثارة الاضطراب فيها، أو تجنّب ذلك الأمر. وعلى الرغم من أنّه فارق كبير، فإنه من الممكن تأخيره شـهوراً أو حتى سـنين. ولأنّ اختراق شـبكات بلد ما يؤثـر في نطاقه الإقليمي، فمن شـبه المؤكّد أن يكون غير شرعي بموجب قوانين ذلك البلد. وعلى الرغم من ذلك، تستمر البلدان في اختراق شبكات بعضها بعضاً.

هنـاك مثـال على ذلك. في 2012، اخترقـت «وكالة الأمن القومـي» تكراراً البنية التحتيّة للإنترنت في سوريا. وقصدت الوكالة من ذلك زرع برنامج شيفري للتنصّت في أحـد المحوّلات الأساسـيّة لشـبكة الإنترنت في ذلـك البلد، لكن الوكالة تسـبّبت عرضاً في انقطاع الإنترنت عن البلد بأكمله[126]. إنّ ضرب شبكة الإنترنت في بلد ما أو محاولة استخراج ملفات منها، هما أمران يجريان بواسطة العمليات نفسها بالضبط.

تعيـش الحكومـات الزمـن الكبـير للحـرب السـبرانيّة في الفضـاء الافـتراضي. وتمتلك 30 بلداً قواتٍ للحرب السبرانيّة في جيوشها[127]، هي: الولايات المتّحدة، روسـيا، الصين، معظم بلدان الاتّحاد الأوروبي، إسرائيل، الهند، البرازيل، أستراليا، نيوزيلنـدا، ومجموعة من البلدان الأفريقيّة. في الولايات المتّحدة، يقود تلك القوّات «المركز الأميركي لقيادة الحرب السـبرانيّة» في وزارة الدفاع. ويتولىّ الأميرال مايكل

(*) هـي مناطـق في الشـيفرة الإلكترونيّة للبرامج يجـري توهينها عمداً، لتسـهيل التعـرّف إلى منظومتها واختراقها، ثم الدخول منها إلى بقية الشيفرة.

إس. روجرز قيادة القوّات السبرانيّة و«وكالة الأمن القومي» معاً. ويظهر ذلك مدى تقارب المهمتين.

ثمة أمثلة قليلة معروفة عن قدرة الهجمات السبرانيّة في التسبّب بأذى فعليٍّ في الأرواح أو الممتلكات. في 2007، وقعت أستونيا ضحية لسلسة واسعة من الهجمات السبرانيّة[128]. غالباً ما يشار إلى ذلك باسم «الحرب السبرانيّة الأولى»؛ نظراً لترافقه حينها مع تصاعد التوتر بين أستونيا وجارتها روسيا. وقعت جورجيا، وهي جمهوريّة سوفياتيّة سابقة، ضحية لسلسلة من الهجمات السبرانيّة التي سبقت بعام غزواً برياً للقوات الروسيّة[129]. في 2009، كانت كوريا الجنوبيّة ضحيّة هجمات سبرانيّة[130]. وشُنّت تلك الهجمات كلها بأسلوب «منع الخدمة»، الذي يرتكز إلى ضخّ كميات ضخمة من المواد والملفات الرقميّة إلى المواقع المستهدفة، إلى حدّ «إتخامها» وشل قدرتها على العمل بصورة مؤقّتة. إنّها ضربات مثيرة للاضطراب، لكنها لا تحدث أذىً عميق الغور، على المدى الطويل.

في تلك الهجمات عينها أيضاً، لم تتوافر أدلّة مؤكّدة على هويّة المعتدي، ولا حتى إذا كان جهة حكوميّة أم لا. في 2009، نُسِبَت الهجمات على أستونيا إلى مجموعة شبابيّة مؤيّدة للكرملين[131]، على الرغم من أنّه لم يُدَنْ أحد رسمياً سوى شاب روسي عمره 22 سنة[132]، من سكان مدينة «تالين»، عاصمة أستونيا. ويندر الوصول إلى ذلك المستوى من التعرّف إلى هويّة منفّذي الهجمات السبرانيّة. وعلى غرار هجمات التجسّس التي نوقشت قبلاً، يصعب تتبع الهجمات السبرانيّة. ويُترَك لنا أن نحدس بهوية المعتدي استناداً إلى قائمة الضحايا. في حال وجود توتّرات إثنية مع روسيا، تنسب الهجمات إلى روسيا بالطبع. إذا هوجمت كوريا الجنوبيّة، فمن غير كوريا الشماليّة قد تحرّك لمهاجمتها؟

يعرّف الفيروس الإلكتروني «ستاكس نت» (Stuxnet) بوصفه أول سلاح سبراني بمستوى عسكري[133]. أطلق في 2009 من قِبَل الولايات المتّحدة

وإسرائيل كي يضرب منشأة «نطنز» النوويّة في إيران، ونجح في إحداث أضرار مادية مباشرة[134]. وشهد العام 2012، هجمة سبرانيّة استهدفت منشأة «آرامكو» السعودية، في ما يعتقد بأنّه رد إيراني[135].

شبكة مفردة للرقابة الدوليّة الشاملة

هنالك قوة دفع نحو الاحتكار تتولّد من الرقابة الإلكترونيّة الشاملة. في مطلع هذا الفصل، تحدّثت عن الفارق بين تجسّس الحكومات على بعضها بعضاً، والرقابة الحكوميّة على الشعب. وبشكل أساسي، يسير التجسّس الحكومي وفق خطوط السياسة، وتتآزر بلدان متحالفة في التجسّس على أعدائها. وفعلنا ذلك أثناء «الحرب الباردة». إنّها السياسة.

تمثّل الرقابة الشاملة أمراً مختلفاً. إذا كنت قلقاً حقاً من إمكان أن تأتيك هجمات من أي شخص وأي مكان، تشعر بالحاجة إلى التجسّس على كل شخص في كل مكان. ولأن لا بلد يستطيع فعل ذلك وحده، يبدو منطقيّاً التشارك في المعلومات مع بلدان أخرى[136].

لكن، مع من تتشارك في معلوماتك وبياناتك؟ بإمكانك أن تتشارك مع حلفائك عسكريّاً، لكنهم ربما لا يتجسّسون على بلدان تهتم أنت بها. وربما كانت مستوى رقابتهم لكوكب الأرض وسكانه، لا تلبي هواجسك بشكل كافٍ، فلا تبدو مشاركتك إياهم المعلومات أمراً مجدياً. يكون من الأفضل منطقيّاً أن تتشارك[137] مع دولة تملك شبكة التجسّس الأكثر اتّساعاً في العالم: الولايات المتّحدة.

تصف تلك الكلمات ما يجري حاضراً. إذ تتشارك الاستخبارات الأميركيّة مع بلدان عدّة. هناك تشارك بين بلدان صديقة لبعضها بعضاً، وتتمتع بالثروة وتتكلم الإنكليزيّة، وتسمّى «العيون الخمس» (Five Eyes)[138]: الولايات المتّحدة، المملكة المتّحدة، كندا، أستراليا، ونيوزيلندا. وتضم شراكة «العيون التسع»[139] البلدان

الخمسة السابقة، إضافة إلى فرنسا، والدانمارك، وهولندا، والنرويج. وتشمل شراكة الـ «14 عيناً»[140] البلدان التسعة السابقة، إضافة إلى ألمانيا، وبلجيكا، وإسبانيا، وإيطاليا، والسويد[141]. وتتشارك الولايات المتّحدة مع بلدان محافظة تقليديّاً كالهند وباكستان، إضافة إلى نُظُم قمعية أخرى (...)[142].

تعطي تلك البلدان كلها لـ «وكالة الأمن القومي» الحق في الوصول إلى كل شيء تقريباً[143]. في شهادة تقدّم بها إلى الاتّحاد الأوروبي في 2014، أورد سنودن أنّه «بالنتيجة، هناك «بازار» أوروبي ربما يقدّم فيه بلد عضو في الاتحاد الأوروبي كالدانمارك، إلى «وكالة الأمن القومي» الحق في الوصول إلى كل شيء مع وضع شرط (غير ملزم) بعدم رقابة الدانماركيّين؛ كما قد تعطي ألمانيا حقّاً مشابهاً إلى «وكالة الأمن القومي» شرط عدم رقابة الألمان. ولكن، من الممكن أن يكون مركزا اختراق الإنترنت (أحدهما بمشاركة ألمانيا والآخر الدانمارك)، عبارة عن نقطتين على الكابل نفسه. وبذا، تحصل «وكالة الأمن القومي» على معلومات عن المواطنين الألمان عندما تمرّ حركتهم على الإنترنت بالدانمارك، وتحصل على معلومات عن المواطنين الدانماركيّين عند مرور حركتهم على الإنترنت بألمانيا؛ فيما يعدُّ ذلك كله متوافقاً تماماً مع الاتفاقيّات الموقّعة مع البلدين».

في العام 2014، صرنا نعرف أن «وكالة الأمن القومي» تتجسّس على الحكومة التركيّة، فيما تتشارك في الوقت عينه مع تركيا للتجسّس على المتمرّدين الأكراد في تركيا[144]. وكذلك علمنا أنّ «وكالة الأمن القومي» تتجسّس على أحد أكثر شركاء الرقابة قرباً منها: ألمانيا[145]. ويسود اعتقاد بأننا نتجسّس على شركائنا جميعهم[146]، فيما عدا الشركاء الأربعة في «العيون الخمس». وحتى عندما تتفاخر «وكالة الأمن القومي» بنجاحاتها في مكافحة الإرهاب[147]، يكون معظمها تهديدات أجنبيّة كانت موجّهة ضد بلدان أجنبيّة، بمعنى أنها لا تتعلّق بالولايات المتّحدة.

ليـس أمراً مفاجئاً القـول إن الولايات المتّحدة تتشـارك المعلومات مع إسرائيل. وتقليديّـاً، تـزال أسـماء الأميركيّـين قبـل المشـاركة في المعلومـات بـين الولايـات المتّحـدة وبلدان أخرى، بهدف حمايـة أمن الأميركيّين. لكن، يبـدو أن إسرائيل تمثّل اسـتثناءً. إذ تعطـي «وكالة الأمن القومـي» إسرائيل «الوحـدة 8200» السريّة التي تتضمّن «سـيغينت الخام» (raw SIGINT)[148]، وهي النظام السري للإشـارات في الاستخبارات الأميركيّة.

حتى الأعداء التاريخيون لأميركا يتشـاركون المعلومات والبيانات معها، ولو أنّ ذلـك يجري ضمن نطـاق ضيّق[149]. بعد هجمات 9/ 11، أعادت روسـيا تصنيف الانفصاليّـين الشيشـان بوصفهـم إرهابيّين، وأقنعـت الولايات المتّحـدة بأنّها تقدم مسـاعدة بالتشارك في المعلومات[150]. في 2011، حذّرت روسيا الولايات المتّحدة مـن تامرلان تسـارناييف، مفجّر سـباق ماراثـون بوسـطن[151]. وردّت الولايات المتّحدة الجميل بفرض رقابة على التهديدات في «دورة سوتشي الأولمبيّة»[152].

لا تبدو تلك المشـاركات منطقيّة إذا نُظر إليها من زاوية تجسّـس الحكومات على بعضهـا بعضاً، لكنها تغدو واضحة وملائمة عندما يكون هدفها الرئيس هو الرقابة العامة. وبذا، ففيما تعلن ألمانيا غضبها من تجسّس «وكالة الأمن القومي» على قادتها، يسـتمر جهازهـا للاسـتخبارات «بي آن دي» (BND) في التعـاون مـع «وكالة الأمن القومي» لرقابة الآخرين جميعهم.

ليست محصلة تلك الأمور كلها سارة أبداً، بل تتمثّل في نسج شبكة عالميّة شاملة، تتواطأ فيها الدول لرقابة كل شخص على الكرة الأرضيّة. ربما تأخّرت تلك الشبكة في الظهور لفترة ما، فهناك بلدان ما زالت خارجها كروسـيا التي تصرّ على فعل كل شيء بنفسـها، وكذلـك تحول الخلافات الأيديولوجيّة الصلبـة دون أن تتعاون دولة كإيران مع روسـيا أو الولايات المتّحدة؛ لكن معظم البلدان الصغيرة سـتجد أسباباً للانخـراط في تلك الشـبكة. ومن وجهـة نظر ضيّقة تماماً، ربـما كان ذلك هو الشيء المنطقي الذي يجب القيام به.

6

تعزيز السيطرة المؤسّساتيّة

لا تنفصل رقابة الحكومة عن نظيرتها لدى الشركات. إنّهما متشابكتان في نسيج واحد، وتعتمد إحداهما على الأخرى. إنّها شراكة القطاعين العام والخاص التي تطوف بالعالم. إنّها ليست اتفاقيّة رسميّة، بل تحالف مصالح[1]. وعلى الرغم من أنها ليست مطلقة، فإنها صارت حقيقة مسلّماً بها، مع سعي لاعبين أقوياء من الممسكين بالمصالح فيها إلى جعلها تستمر إلى الأبد. وعلى الرغم من أن وثائق سنودن عن رقابة «وكالة الأمن القومي» أحدثت شروخات في تلك الشراكة، وهو أمر سأتناوله في الفصل 14، فإنّها ما زالت قويّة.

أوضحت وثائق سنودن مدى اعتماد «وكالة الأمن القومي» على الشركات الأميركيّة في التجسّس على الإنترنت. إذ لم تبنِ «وكالة الأمن القومي» نظام التنصّت على الإنترنت من لا شيء. لاحظت الوكالة أن عالم الشركات أنجز بناء ذلك النظام، فاخترقته واعتمدت عليه. وبواسطة برامج كـ «بريزم» (PRISM)، أرغمت «وكالة الأمن القومي» شركات كـ«مايكروسوفت» و«غوغل» و«آبل» و«ياهوو»، على إمدادها ببيانات عن بضع آلاف من الأشخاص الذين اهتمت بهم الوكالة. وبواسطة برامج أخرى، حصلت «وكالة الأمن القومي» على نفاذ مباشر إلى التركيب الأساسي للإنترنت[2]؛ كي تمارس رقابة واسعة شملت الجميع. وأحياناً، تعاونت تلك الشركات مع الوكالة طوعيّاً. وفي أحيان أخرى، أرغمتها المحاكم على

تسليم البيانات والمعلومات، غالباً بطريقة سريّة. في أحيان أخرى، اخترقت الوكالة البنية التحتيّة الإلكترونيّة للشركات، من دون الحصول على إذن من الأخيرة.

يحدث ذلك في العالم بأجمعه. إذ تستخدم دول عدّة قدرات الرقابة لدى الشركات كـي تراقب مواطنيها. وبواسـطة برنامـج كـ «تمبـورا» (TEMPORA) تدفع «القيادة الحكوميّـة للاتّصالات» في المملكة المتّحـدة، إلى شركات اتّصالات كـ«بي تي» (BT) و«فودافـون» (Vodafone) [3]؛ كي تعطيها منافذ إلى الكتل الرئيسـة للاتّصالات في العـالم بأكمله. وتقدّم «فودافون» إلى حكومـات ألبانيا، ومصر، وهنغاريا، وإيرلندا، وقطـر (وربما مـا مجموعه 29 بلـداً)، منافذ للدخول مبـاشرة إلى حركة الإنترنت في بلدانهـا[4]. ولا نعـرف إلى أي مـدى تدفع تلك الحكومات لقـاء منافذ الدخول على الاتّصالات والإنترنت، كما تفعل المملكة المتّحدة أيضاً، أم إنها تحصل عليها بمجرد طلبهـا. وتتنصـت الحكومة الفرنسـيّة على «فرانـس تليكـوم» (France Télécome) و«أورانـج» (Orange) [5]. سـبق أن تحدّثنا عن الصين وروسـيا في الفصل 5. تحوز عـشرات البلدان قوانين عن الاحتفاظ بالمعلومـات[6]- أعلن الاتحاد الأوروبي أنها تعـدُّ غـير دسـتوريّة في 2014 - تفـرض عـلى مقدّمي خدمـة الإنترنـت الاحتفاظ بالبيانات المتعلّقة بزبائنها بضعة شهور، كي تراجعها الحكومة في حال رغبت بذلك. ويجـب على مقاهي الإنترنت في إيـران[7]، وفيتنام[8]، والهنـد[9]، وغيرها، الحصول على معلومات عن هويّات مستخدميها والاحتفاظ بها.

تحدث أشـياء مماثلة خارج الإنترنت. ومباشرة عقب 9/ 11، اشـترت الحكومة الأميركيّة بيانات من سماسرة المعلومات[10]، شملت الحصول على بيانات المسافرين جوّاً من شركة «تورش كونسبتس» (Torch Concepts) [11]، وقاعدة بيانات الناخبين المكسـيكيّين مـن شركـة «تشـويس بوينـت» (ChoicePoint) [12]. يفـرض القانون الأميركي على المؤسّسـات الماليّة تقديم تقارير للحكومة عن المعاملات النقديّة التي تزيـد قيمتهـا على عـشرة آلاف دولار[13]، وينخفض الرقـم إلى ألف دولار في حال صرف عمـلات أجنبيّـة. تفرض مجموعة مـن الحكومات على الفنـادق الإبلاغ عن

الأجانـب الذين يقضون ليلة فيها، فيما تفـرض مجموعة أكبر من الأولى على الفنادق الحصول على نسـخ من بطاقات الهويّة وجوازات السـفر للنزلاء الأجانب. وكذلك تسـتعمل كثير مـن الحكومات كامـيرات الرقابة في الأمكنـة العامـة، ونُظُم تصوير لوحات المركبات، و«البيانات المكانيّة» للخلوي.

وفي السـياق عينـه، تحصـل الـشركات عـلى معلومـات حكوميّـة وتسـتعملها لمصلحتها. إذ تبيع ولايات كـإيلينوي[14] وأوهايو[15] وتكساس[16] وفلوريدا[17]، بيانات عن رُخص قيادة المركبات تشـمل الصور، إلى شُراة من القطاع الخاص. تبيع ولايات أخرى بيانات تسجيل الناخبين[18]. في 2014، اقترحت الحكومة البريطانيّة بيـع بياناتها عن ضرائـب الدخل[19]، لكـنّ احتجاجاً عموميّـاً أدى إلى تأجيل تلك الخطـوة، مؤقّتاً على الأقل. وتزمع «الخدمات الصحيّـة الوطنيّة» في المملكة المتّحدة، بيع البيانات الصحيّة للمرضى إلى شركات الأدوية والتأمين الصحي[20]. ثمة حلقة من التغذية الراجعة[21]: تناقش الشركات لمصلحة الحق في الحصول على المعلومات مـن الحكومـة، ثم تحاجج بأن تلك المعلومات يجـب أن توضع تحت قوانين حكوميّة مفتوحة، وبعد ذلك؛ تعلّب الشركات المعلومات كي تبيعها إلى الحكومة مجدّداً.

وتكـون النتيجة النهائيّة تداول كميّات كبيرة من بيانـات الرقابة ومعلوماتها بين الشركات والحكومات. وكذلك تكون إحدى النتائج المباشرة لتلك العملية صعوبة تمريـر قوانـين فعّالة للجـم رقابة الشركات؛ ذلـك أن الحكومات لا ترغـب فعليّاً في تقييد حصولها هي نفسها على البيانات والمعلومات بلجم ممارسة الشركات للرقابة، طالما أن الأخيرة تمدّ الحكومات ببيانات عنها.

يصلح النقاش عن شـعار «لا تتعقّب» نموذجاً قويّـاً عن رداءة الوضع حاضراً. فلسـنوات طويلـة، حاول نشـطاء الدفاع عـن الخصوصيّـة تمرير قانـون يفرض أن يُعطـى مسـتخدمو الإنترنت خياراً يمكّنهم من تهيئة محـرّكات البحث بما يحول دون تتبعّهـم من قِبَل المواقـع التي يزورونها عـلى الإنترنت[22]. اقترَحَـت مجموعة كبيرة

مـن القوانـين الوطنيّة في الولايات المتّحدة عن ذلك الأمـر، لكن شركات الإنترنت قاومتهـا بـضراوة، ولم يمـرَّر أي قانـون في ذلك الشـأن. وفي 2013، مـرّرت ولاية كاليفورنيا قانوناً من ذلك النوع، لكن مجموعات الضغط خفّفته مراراً وتكراراً حتى باتت منفعة مستخدمي الإنترنت منه ضئيلة للغاية. ووفق ذلك القانون، تملك الحق كمسـتخدم في إبلاغ المواقع بأنك ترغب في ألا تُلاحَق على الإنترنت، ولكن المواقع تملك الحق أيضاً في تجاهل رغباتك.

تختلـف الأمـور قليـلاً في أوروبـا[23]. هنـاك قانـون كـ «التوجيـه بشـأن حمايـة البيانـات»، يفرض قيـوداً أكبر على رقابـة الشركات، وقد أحدث بعـض التأثير. في المقابـل، جرى التوقيع على «معاهدة الملاذ الآمـن»(*) (Safe Harbor) بين الولايات المتّحـدة والاتحاد الأوروبي، وهي تعني أن البيانات والمعلومات الشـخصيّة يمكنها أن تتدفّـق مـن الاتحـاد الأوروبي إلى شركات المعلوماتيّـة الأميركيّـة في الولايـات المتّحدة[24]، التي تفرض قيوداً أقل تشدّداً من تلك التي يطبّقها الاتحاد الأوروبي.

شراكة القطاعين العام والخاص في الرقابة[25]

لا تمـارس الحكومـات الرقابـة والحجـب والتحكّـم بالعمليّات على الشـبكات بواسـطة أجهزتها وحدهـا؛ إذ تلقى دعماً من شراكة واسـعة في الرقابة بين القطاعين العـام والخـاص، يتمثّل في مروحة مـن الشركات السـاعية للربـح. في 2010، بيّن تحقيـق أن 1931 شركـة مختلفـة داخـل الولايات المتّحـدة تعمل في الاسـتخبارات ومكافحـة الإرهاب وأمن الوطن[26]. وفي مقال ظهر عام 2013، أوردت صحيفة **واشنطن بوست** أن 70 ٪ من ميزانية الاستخبارات في الولايات المتّحدة تذهب إلى شركات خاصـة[27]، وأنّ 483 ألـف متعاقد مع الحكومـة يملكون تراخيص سريّة جـداً، وهم ثلث عـدد أصله 1.4 مليـون متعاقد مع الاسـتخبارات. في ذلك، تبرز

(*) عنـد ترجمـة الكتـاب، كانت معاهدة لم يكشـف الطرفان تفاصيلها، اسـم "برايفسي شـيلد" (Privacy Shield)، حلّت بديلًا لهذه المعاهدة التي ألغتها «محكمة العدل الأوروبيّة» أواخر 2015.

بوضوح سياسة «الباب الدوّار» في العلاقة بين الحكومة والشركات المتعاقدة معها في الاستخبارات.

غادر الأميرال مايك ماكّونيل «وكالة الأمن القومي» بعد أن ترأسها بين عامي 1992 و1996، ليصبح نائباً لرئيس شركة «بووز آلن هاملتون»(*) (Booz Allen Hamilton) مستمراً في العمل على مسائل تتعلّق بالأمن القومي.

وبعد أن تقاعد من إدارة «وكالة الأمن القومي» في 2013، أنشأ كييث ألكسندر شركة مختصّة بالاستشارات عن أمن الإنترنت[28]، وحصل على براءات اختراع عن تقنيّات في الأمن زعم أنها طُوّرَت زمن ولايته. ووظّف في شركته المدير الرئيسي للتكنولوجيا في «وكالة الأمن القومي» مع استمرار الأخير في العمل ضمن الوكالة[29].

تبيع مجموعة من الشركات الصانعة للأسلحة السبرانيّة أدوات لاختراق الشبكات إلى حكومات عدّة. ومثلاً، يوصف برنامج «فِن فيشر» (Fin Fisher) [30] من قبل شركته الصانعة «غاما غروب» (Gamma Group) الألمانيّة- البريطانيّة، بأنّه «حلّ معلوماتي هجومي للاقتحام». وتشتري حكومات عدّة ذلك البرنامج كي تتجسّس على حواسيب الناس وهواتفهم الذكيّة. في 2012، عثر بحّاثة على أدلة عن استخدام «فِن فيشر»[31] في البحرين وسنغافورة وأندونيسيا ومنغوليا وتركمانستان ودولة الإمارات العربيّة المتّحدة وإثيوبيا وبروناي، إضافة إلى الولايات المتّحدة وهولندا.

في الفصل 5، تناولت المجموعة الإيطاليّة «هاكينغ تيم». وتستعمل أدواتها الرقميّة المخصّصة لاختراق الكومبيوتر والخلوي الذكي ومنتجاتها الإلكترونيّة للرقابة من قِبَل حكومات: أذربيجان وكولومبيا ومصر وإثيوبيا وهنغاريا وإيطاليا وكازاخستان وكوريا وماليزيا والمكسيك والمغرب ونيجيريا وعُمان وبنما

(*) عند ترجمة الكتاب، كان اسم الشركة قد تغيّر إلى "استراتيجي أند" (Strategy &).

وبولندا والسعوديّة والسودان وتايلاند وتركيا ودولة الإمارات العربيّة المتّحدة وأوزبكستان. ووظّفت الحكومة المغربيّة[32] برامج «هاكينغ تيم» لاستهداف مجموعة تنشط ضمن ما يعرف باسم «صحافة المواطن» الإلكترونيّة وتحمل اسم «مامفاكينش»، بواسطة رسالة بريد إلكتروني زعمت أنها من مواطن مهدّد بالخطر؛ لكن الملف المرفق بالـ «إيميل» كان محمّلاً بالبرنامج الخبيث لشركة «هاكينغ تيم».

في العام 2011، أُظهِرت لمتمردين اعتُقِلوا في البحرين نصوص من رسائلهم في الـ «إيميل» وجلسات «الدردشة» على الإنترنت، عملت الحكومة على جمعها بواسطة أدوات رقميّة حصلت عليها من شركتي «نوكيا» و«سيمنز»[33].

هناك أيضاً مؤتمر «عالم آي إس إس» (ISS World)[34]، اختصاراً لاسم «نُظُم دعم الذكاء» (Intelligence Support Systems)، الذي يدأب على إقامة معارض تجاريّة في مدن كدبي وبرازيليا. وفي منشوره الدعائي لمعارض العام 2014[35]، أعلن الـ «آي إس إس» تخصيصه جلسات عن الرقابة المكانيّة، والتفتيش في سجلات المكالمات الهاتفيّة، والاقتحام المعلوماتي الهجومي، وطرق كسر الشيفرة؛ فيما ضمّت قائمة الشركات الراعية للمؤتمر نخبة الشركات التي تنتج تلك القدرات في الرقابة. ترسل بلدان عدّة ممثلين عنها كي يحضروا ذلك المؤتمر[36]، الذي يوجد أكثر من نظير له في أوروبا والولايات المتّحدة[37].

تعمل كبريات شركات الأسلحة المتعاقدة مع الجيش الأميركي[38]، كـ «رايثيون» (Raytheon) و«نورثروب غرومان» (Northrop Grumman) و«هاريس كوربوريشن» (Harris Corporation)، على صنع أسلحة سبرانيّة للجيش الأميركي. وتساعده مجموعة من كبرى شركات المعلوماتيّة في إنشاء مراكز للرقابة الإلكترونيّة في أرجاء المعمورة. وساعدت الشركة الفرنسيّة «بول إس إيه» (Bull SA) الحكومة الليبيّة في بناء مراكز للرقابة[39]. واستخدمت نيجيريا شركة «إلبايت سيستمز» (Elbeit Systems) الإسرائيليّة[40]. واستعملت الحكومة السوريّة شركة

«سيمنز» الألمانيّة[41]، وشركة «إيريا إسبي إيه» (Area SpA) الإيطاليّة[42] وغيرهما. واشترى نظام معمّر القذافي في ليبيا نظاماً للرقابة على الهواتف النقّالة من شركتي «زد تي إيه» الصينيّة و«فاس تيك» (VASTech) الجنوب أفريقيّة[43]. ولا نعرف من بنى نظم رقابة الإنترنت في أذربيجان[44] وأوزباكستان[45]، لكن من شبه المؤكّد أن شركات غربيّة ساعدتها في ذلك.

هنالك عدد قليل من القوانين التي تمنع نقل تقنيّات الرقابة، ومعظمها يجري تخطّيه بسهولة[46].

لا تنحصر تلك التقنيّات بنُظُم مصمّمة خصيصاً للتنصّت الحكومي، بل إنّ معظم البنيّة التحتيّة للرقابة الحكوميّة بُنِيَتْ كي تستخدمها الشركات[47]. تبيع الشركة الأميركيّة «بلو كوت» (Blue Coat) نُظُماً تقنيّة للترصد ورقابة المحتوى إلى شبكات تستعملها الشركات، كما تُستَخْدَم أيضاً في الرقابة الحكوميّة في بلدان كبورما، والصين، ومصر، وأندونيسيا، ونيجيريا، وقطر، والسعودية، وتركيا، وفنزويلا[48]. ويستعمل برنامج تنتجه شركة «نتسويبر» (Netsweeper) الكنديّة لرقابة المحتوى، من قِبَل جهات الرقابة الحكوميّة في قطر، واليمن، ودولة الإمارات العربيّة المتّحدة، والصومال، وباكستان[49]. وكذلك يستعمل برنامج رقابة المحتوى الذي تصنعه شركة «فورتينت» (Fortinet) الأميركيّة، لفرض حجب على مواقع للإنترنت في بورما[50]. وهناك برنامج مشابه اسمه «سمارت فلتر» (SmartFilter) تصنعه شركة «ماكافي» (McAfee) الأميركيّة، يستخدم بصورة طبيعيّة في المدارس، ساعد حكومات تونس وإيران في فرض حجب على مواقع الإنترنت في البلدين[51]. واستُخدمت معدّات تصنعها شركة «سوفوس» (Sophos) البريطانيّة، لفرض رقابة على المواطنين واعتقالهم، من قبل سوريا وعدد من النُظُم القمعيّة الأخرى.

ثمة حياد في التكنولوجيا حيال القيم. إذ بإمكانك استعمال الخلوي في طلب النجدة لأناس في حالات طارئة، أو لوضع تخطيط لسرقة بنك. لا يوجد فارق

تقني بين استخدام حكومة لأداة معلوماتيّة في التعرّف إلى مجرمين، أو استعمالها للتعرّف إلى منشقين عنها. لا يوجد فوارق تقنية في استعمال حكومة لأداة معيّنة أو استخدامها من قِبَل شركة. كذلك فإنّ الأدوات الرقميّة التي تستعملها الشركات بصورة قانونيّة لرقابة «إيميل» موظّفيها كي لا يسرّبوا أسرارها، يمكن استعمالها أيضاً من قِبَل حكومات قمعيّة بهدف الرقابة والحجب. وعلى العكس من ذلك، فإن الأدوات التقنيّة عينها التي يستخدمها المنشقون الإيرانيّون والسعوديّون للتهرّب من الحجب الحكومي، يمكن استعمالها أيضاً من قِبَل مجرمين يسعون لنشر أفلام إباحيّة تستغل الأطفال جنسيّاً. ويسمح التشفير للأشخاص الطيّبين بالتواصل مع الأشرار، لكنها تسمح للشريرين أيضاً بأن يتواصلوا من دون أن يتنصّت عليهم الأشخاص الطيّبون[52]. وهناك تقنيّات للتعرّف إلى الوجوه تستعملها شركة «ديزني» في منتجعاتها لالتقاط صور مديريها مع الزوار كهدايا[53]، ومن المستطاع استعمالها للتعرّف إلى وجوه المحتجين السياسيّين في الصين، ونشطاء حركة «احتلوا وول ستريت» (Occupy Wall Street) في نيويورك.

الحكومات تخرّب الشبكات التجاريّة

حتى هذه النقطة، ناقشتُ كيف تستفيد رقابة الحكومات من القدرات التقنيّة للشركات. وتبدو تلك الصورة صحيحة في معظمها، ولكن لا تنأى الحكومات بنفسها أيضاً عن إرغام الشركات على التجسّس لمصلحتها.

في مطالع التسعينيات من القرن الماضي، شرعت الـ «إف بي آي» في الإعراب عن قلقها من قدراتها في الرقابة على الهواتف. درجت الـ «إف بي آي» على إتمام تلك الرقابة في عصر المحوّلات القديمة للهواتف الأرضيّة، بجهود تتضمن غرس الملاقط في الخطوط، والتلاعب بأسلاك الخطوط، والتسجيلات على أشرطة النايلون الممغنطة. تمثّلت المشكلة حينها في أن المحوّلات الهاتفيّة لا تعمل بتلك الطريقة. وبدا أنّ عزل رقم هاتفي بعينه أمر صعب، ما أثار قلق «إف بي آي» من

إمكان أن تفقد قدرة التنصّت على المكالمات. ولذا، مارست ضغوطاً متصاعدة على الكونغرس، وحصلت في 1994، على تشريع اسمه «قانون مساعدة الاتّصالات في إنفاذ القانـون» (Communications Assistance for Law Enforcement Act)[54]، واشتُهِر باسـمه المختـصر «كاليـا» (CALEA)، يفـرض عـلى شركات الاتّصـالات تصميم محوّلاتها الرقميّة بما يجعل القدرة على التنصّت جزءاً أساسيّاً مثبّتاً فيها.

وبالقفز 20 سـنة إلى الأمام، نرى أن الـ «إف بي آي» تريد مرّة أخرى من صناعة المعلوماتيّـة والاتّصالات المتطوّرة أن تسـهّل لها مهمـة الرقابة. لم يعد جزء كبير من الاتّصـالات يُجـرى بواسـطة الهاتف، بـل بالتحـادث في مواقع الإنترنـت، والبريد الإلكتروني وموقع «سكايب». وحاضراً، تمارس الـ «إف بي آي» ضغوطاً للحصول عـلى تحديـث لقانـون «كاليا»[55]، بـما يجعله قادراً عـلى تغطية الاتّصـالات المتطوّرة بأنواعهـا كافـة: المكالمـات الصوتيّـة، والأشرطـة والصـور، والنصـوص المكتوبة، وألعـاب إلكترونيّة كـ «وورد أوف ووركرافت»، وتلك النافذة الصغيرة للدردشـة مع بقية المشاركين في لعبة «سكرابل» عبر الإنترنت.

يتمثّـل الهـدف النهائـي للـ «إف بي آي» في حظـر الاتّصالات الآمنـة كافة[56]. ويصيـغ فالـيري كابروني، المستشـار العام للـ «إف بي آي» الأمر عـلى النحو التالي: «يجب ألا يَعِدَ أحدٌ المستهلكين بأنهم لن يُجلَبوا إلى المحاكم الأميركيّة. من المسـتطاع وعد الناس بالحصول على تشـفير قوي، لكن يجـب عليهم أيضاً أن يفكروا في كيفيّة إيصـال النـص الأصـلي الواضـح إلى أيدينـا». وتترجم تلـك الكلمات بـأنّ أحداً لا يستطيع إمداد جمهور الزبائن باتّصالات آمنة فعليّاً.

واعتـماداً عـلى نـوع النظـام، يتـدرّج إنجاز ما تسـعى إليـه الـ «إف بي آي»، من السـهل إلى المسـتحيل. في نُظُم كالبريد الإلكتروني «جي ميل»، يكون الأمر سـهلاً. إذ تتراكم الرسـائـل غير المشـفّرة في خوادم شركة «غوغل»، وتملك الشركة مكتباً بطواقم جاهزة للرد على طلبات الدخول إلى الرسـائل الشـخصيّة من حكومات في

أرجاء العالم. وتبدو برامج تشفير المحادثات من نوع «أوف ذي ريكورد» (Off the Record)، عصيّة على الاختراق، كما أنها لا تستخدم عقدة مركزيّة لاتّصالاتها كي يجري التنصّت عليها. في تلك الحالات، يكون الحلّ الوحيد لتلبية مطالب الـ«إف بي آي» هو زرع «باب خلفي» في برنامج المستخدم، ما يجعله قابلاً للاختراق من قِبَل الجميع. سوف أتناول مدى غباء تلك الفكرة في الفصل 11.

وعلى الرغم من الطغيان الذي يتّسِم به ذلك الإجراء، فإنّ نقاشاً عاماً شرع يثور حوله، على الأقل. وغالباً، تسري هيمنة الحكومات على البنية التحتيّة لاتّصالات الشركات، في سريّة عالية، فلا نسمع بها إلا بالمصادفة.

كانت «لافابيت» (Lavabit) من الشركات التي قدّمت حماية للخصوصيّة أكثر مما تفعله الشركات الكبرى لخدمات البريد الإلكتروني التي يستخدمها معظمنا. وهي شركة صغيرة للبريد الإلكتروني امتلكها مبرمج اسمه لادار لِفيزون[57]، ولقيت رواجاً بين هواة التقنيّات. بلغ عدد مستخدميها نصف مليون، بينهم إدوارد سنودن.

عقب فرار سنودن إلى هونغ كونغ في 2013، تلقى لِفيزون رسالة من «وكالة الأمن القومي» تطلب الشيفرة التي تستخدمها شركة «لافابِت» في حماية مستخدميها كلّهم- مع عدم إشعارهم بإمكان أن تطالهم الرقابة[58]. خاض لِفيزون معركة ضد تلك الرسالة في القضاء، وعندما بدا جليّاً أنه بصدد الخسارة، فضّل إغلاق شركته على مخادعة زبائنه وعقد صفقة تسوية من وراء ظهورهم.

الخلاصة الأخلاقيّة من تلك القصة واضحة. إذا أسّست عملاً تقنيّاً، فهناك احتمال بأن تحاول الـ«إف بي آي» أو «وكالة الأمن القومي» تحويله إلى أداة للرقابة الجماعيّة؛ لأنها تعتقد أن ذلك من حقّها ووفق شروطها حصريّاً. تستطيع الوكالة أن ترغمك على تعديل نظامك[59]. بإمكان الوكالة أن تفعل ذلك سرّاً، وأن ترغمك على إبقاء ذلك سراً. وعندما تفعل ذلك، تفقد أنت السيطرة على عملك. إذا كنت

مالـكاً لشركة كبيرة، لن تستطيع إغلاقهـا. وواقعيّاً، لا تسـتطيع أن تنهي جزءاً من خدماتـك. بطريقـة واقعيـة تماماً، لم يعـد عملك ملـكاً لك. صار عملـك جزءاً من الذراع القويّة لأجهزة الاستخبارات الأميركيّة؛ وإذا تضاربت مصالحك مع مصالح الوكالة، فلسوف تكسب الأخيرة المعركة. لقد اغتُصِب عملك[60].

يتمثّـل السـبب الوحيد لمعرفتنا تلـك القصة في أن لِفيزون أدار شركته بنفســه. لم يكن لديه أسـياد على شركته، ولا مالكو مصالــح فيها. كان لِفيزون قادراً على تدمير عملـه بنفســه، اسـتناداً إلى أسـباب أخلاقيّـة. لا تسـتطيع الشركات الأكـبر حجماً، والمسـتحوذة من قِبَل كثيريـن، الإقدام على ذلك. يجدر بنا افـتراض أن كل شركات الكومبيوتر التي تلقت طلباً مماثلاً، خضعت في النهاية لما طُلِبَ منها.

مثلاً، نعرف أنّ حكومة الولايات المتّحدة أقنعت «سكايب»- بالرشوة والإرغام والتهديد والقهر القانوني- بإدخال تعديلات على طريقة عمل برنامجها؛ كي تسـهل عمليـات التنصّـت عليـه[61]. لا نعرف ما كانته تلـك التغيـيرات، ولا إذا ما كانت أُدخلَت قبل امتلاك «سـكايب» من قِبَل «مايكروسوفت» في 2011 [62]، ولا حتى إذا كانت كافية بالنسبة لمطالب الحكومة، لكننا نعرف أنّها حدثت[63].

في 2008، هـدّدت حكومـة الولايات المتّحدة موقع «ياهـوو» سراً بتغريمه ربع مليـون دولار يوميّـاً، مع زيـادة ذلك المبلـغ يوميّاً، مـا لم ينضمّ إلى برنامـج «بريزم» (PRISM) الـذي تديـره «وكالـة الأمـن القومـي»[64]. وفي 2004، دفعـت «وكالة الأمـن القومي» إلى شركة «آر إس إيه» لأمن المعلومات، مقابل وضع «باب خلفي» للدخول إلى بيانات توليد الأرقام العشوائيّة في مكتبة نظامها للتشفير[65].

ثمة أنواع أخرى من استيلاء الحكومة عنوة على الأعمال، وتسري راهناً من وراء ظهر الشركات التي يجري تخريب تقنيّاتها في التنصّت. وعندما لا تعقد «وكالة الأمن القومي» اتفاقيّات مع الشركات للتنصّت على نُظُمها، تبذل الوكالة قصارى جهدها كـي يحـدث ذلك بطـرُق خفيّة وملتويـة. ومثلاً، عندمـا لم تكن راضيـة عن كميات

المعلومـات التي تتلقاها من «غوغل» و«ياهوو» بواسـطة برنامج «بريزم»، اخترقت الوكالة الخطوط الرئيسـة للاتّصـالات بين مراكز المعلومـات في الشركتين[66]، ربما بالتعـاون مـع الجهـة التـي منحتهما تلـك الاتّصالات. وظهـر ردّ فعـل غاضب من أحـد مهندسي الأمـن المعلوماتي في «غوغـل»[67]، إذ كتب على صفحته الشـخصيّة في «غوغـل +»، عبـارة: «ليذهب هؤلاء الناس إلى الجحيـم». ومنذ ذلك الحين، لجأ «غوغـل» إلى تشـفير الاتّصـالات بين مراكـز معلوماته سـعياً لإبعـاد الوكالة عنها. ويزعم «ياهوو» أنّه يفعل الأمر نفسه.

ليـس ذلك مثـلاً متفـرّداً عـلى تعمّد «وكالـة الأمـن القومي» اخـتراق شركات التكنولوجيـا. إذ تصنع الوكالة صفحات مزيّفة على «فيسـبوك» لتخترق حواسـيب الناس[68]، ويعمل فرع «تاو» فيها على اعتراض معدّات شركة «سيسـكو سيستمز» أثناء عمليات الشحن؛ كي يدسّ مكوّناته الخاصة فيها[69].

لا نعرف نوع الضغط الذي تمارسـه الحكومة الأميركيّة على المقدّمين الرئيسـيّين لخدمة «حوسـبة السـحاب»، كي تقنعهم بإعطائها منفذاً إلى بيانات مستخدميها، أو إذا كانـت تلك الـشركات أبرمت اتفاقيّات سريّة مع «وكالـة الأمن القومي». لكننا نعلم أن برنامجاً للوكالة اسـمه «بول ران» (Bullrun) يعمل على تفكيك الشـيفرات في الإنترنـت، وأنّ نظـيره البريطاني لدى «القيـادة المركزيّة للاتّصـالات الحكوميّة» يحمل اسـم «إيدج هـل» (EdgeHill). ونجح البرنامجان في هزيمـة معظم إجراءات أمن المعلومات الشـائعة على الإنترنت. هل طلبت «وكالة الأمن القومي» من محرّك البحث «غوغل» المفاتيح الرئيسـة للتشـفير وأرغمته على إبقاء الأمر سراً، كما فعلت مع شركة «لافابِت»؟ هل اخترقت «مجموعة عمليات الدخول المنسّـقة» في الوكالة، خوادم «غوغل» خارج أميركا وسطت على مفاتيح التشفير فيها، أو اعترضت معدّات كانت مرسـلة إلى مراكز للمعلومات يملكهـا «غوغل» خارج أميركا، وزرعت فيها «أبوابـاً خلفيّة» لتسريب المعلومات منها؟ تمثّل تلك الأمور ممارسـات موثّقة تنهض بها الوكالة. في الحال الأولى، يكون «غوغل» قد مُنعَ قانونيّاً من الاعتراف بحدوثها؛ في الحـال الثانيـة، لن يكون «غوغـل» راغباً في الإقرار بحدوثهـا؛ وفي الثالثة، يكون

«غوغل» غير عارفٍ حتى بحدوثها. بصورة عامة، نعرف أنه في السنوات التي تلت 9/ 11، تلقّت الحكومة الأميركيّة سيولاً من التعاون الطوعي معها من شركات اعتقد قادتها أن ما يفعلونه جزء من الواجب الوطني.

أعتقد بأننا سنشاهد مزيداً من الدخول إلى معظم معلوماتنا وبياناتنا، على يد «وكالة الأمن القومي»، بسبب نوع المعلومات التي تسعى إليها. إذ اعتادت الوكالة على الحصول على ما ترغب به الشركات الأساسيّة للإنترنت، ومقدمو خدمات الـ«برودباند» عليها.

أضحى ذلك أقل تحقّقاً لأن التشفير- خصوصاً النوع المسمّى تشفير الـ«إس إس آل» (SSL)- بات أكثر انتشاراً. ويصبح أقل تحقّقاً كلما زادت عمليات التشفير على الإنترنت. للتغلّب على ذلك، تحتاج الوكالة إلى كميات ضخمة من المعلومات المتوافرة لدى الشركات الكبرى لتقديم الخدمات على الإنترنت؛ لأن الشركات تمتلك معلوماتنا وبياناتنا الواضحة غير المشفّرة، فهي تتراكم لديها قبل أن يطالها التشفير. ويتطلّب الحصول على معلوماتنا غير المشفّرة، أن تخرّب الوكالة بروتوكولات الأمن المعلوماتي التي تستعملها مواقع الإنترنت.

هناك دول أخرى منخرطة في ذلك الضجيج المتخالط. ومن المعتقد به على نطاق واسع أنّ الحكومة الصينيّة تدسّ مكوّنات لاستراق المعلومات في كل المعدّات الشبكيّة التي تصنعها وتبيعها شركتها «هواوي». وهنالك أسباب للاعتقاد بأن المنتجات المشابهة التي تصنعها شركات بريطانيّة وروسيّة وإسرائيليّة وفرنسيّة، تتضمن «أبواباً خلفيّة» لتسريب المعلومات، فرضتها حكومات تلك البلدان[70].

لا نعرف إذا كانت الحكومات تحاول بخفاء دسّ «أبواب خلفيّة» لتسريب المعلومات، ضمن منتجات شركات لا تملك حيالها سلطات سياسيّة أو قانونيّة، لكن بعض خبراء الكومبيوتر يعتقدون أن الأمور تحدث على ذلك النحو. هل هناك صينيّون متحمّسون لوطنهم ويعملون في شركات أميركيّة كبرى لبرامج الكومبيوتر

والإنترنت، وهم يسهّلون للحكومة الصينيّة سرّاً اختراق منتجات تلك الشركات؟ أم هُمُ المبرمجون الفرنسيّون؟ أم هُمُ المبرِمجون الإسرائيليّون؟ هل على الأقل يسرّبون شيفرة المصدر إلى بلدانهم، ما يسهّل على الأخيرة العثور على نقاط ضعف فيها؟ هل هناك عملاء أميركيّون يدسّون «أبواباً خلفيّة» في الرقاقات الإلكترونيّة التي تصمّم وتُصنّع في آسيا؟ نعرف أن لديهم موظفيّن مزروعين سراً في بلدان كالصين وألمانيا وكوريا الجنوبيّة[71]؛ كي يساعدوا في زعزعة نُظُم الكومبيوتر والاتّصالات.

استجابت الشركات لتلك الأوضاع باللجوء إلى التطمينات الزائفة المثقلة بالتهديدات القانونيّة. في سياق مؤتمر تكنولوجي في العام 2013، حاول إريك شميدت، المدير التنفيذي لـ «غوغل»، تطمين مستمعيه بالقول إنّه «متأكّد بدرجة كبيرة من أن المعلومات في «غوغل» آمنة حاضراً، وبمنجاة عن العيون الحكوميّة المتفحّصة»[72]. ربما كان أكثر دقة القول: «معلومات بمنجاة عن الحكومة، خلا ما يصيبها بما لا نعرفه من الطُرُق وما لا نستطيع أن نصارحكم بشأنه». ربما بدا ذلك كملاحظة بنبرة لئيمة، لكن طالما كان مسموحاً لـ «وكالة الأمن القومي» أن تستخدم أوامر من المحاكم مستندة إلى تفسيرات سريّة لقانون سريّ، فلن تتبدّل الأوضاع أبداً.

بالنسبة للغالبية العظمى من شركات الإنترنت، لا يمثّل الأمر مشكلة. ما لم يقله إريك شميدت هو: «وبالطبع، نحن نملك أن ننفذ إلى معلوماتكم وبياناتكم كلها، ونستطيع بيعها لمن نرغب... ولا نجاة لكم من ذلك الأمر». وطالما استمرت الشركات في انخراطها في الرقابة العامة للمستخدمين والمستعملين، يكون من الأسهل عليها أن تتجاوب مع طلبات الحكومة والتشارك في تلك الثروة مع «وكالة الأمن القومي».

وطالما استمرت الحكومات في طلب النفاذ إلى المعلومات، ونأت بنفسها عن وضع تشريعات تحمي تلك المعلومات والبيانات، يكون من الأسهل صنع نُظُم تسمح بذلك. هناك دورة تغذية قويّة: يدعم نموذج الأعمال جهود الحكومة، وتبرّر جهود الحكومة نموذج الأعمال.

الجزء الثاني

ما هي الرهانات؟

7

العدالة والحريّة السياسيّة

في العام 2013، رفعت «الكنيسة التوحيديّة الأولى» في مدينة «لوس أنجلوس» دعوى قضائيّة ضد «وكالة الأمن القومي»[1]؛ بسبب تجسّس الأخيرة عليها محليّاً، مشيرة إلى رقابة الوكالة على عادات الاتّصالات الهاتفية لأعضاء الكنيسة، أدّت إلى عزوفهم عن التضامن مع بعضهم بعضاً لدعم قضايا سياسيّة. لم تكن الكنيسة مصابة بالبارانويا ولا بعقدة اضطهاد. ففي خمسينيات القرن العشرين وستينياته، لاحقت الـ «إف بي آي» رئيس كاتدرائيّتها بسبب مواقفه السياسيّة. وحاضراً، تبدي الكنيسة قلقها من شمول أفراد أميركيّين وأجانب في لوائح الرقابة بسبب علاقتهم بتلك الكنيسة[2].

تتكلّف الرقابة الحكوميّة غالياً. وبوضوح تام، تظهر الأرقام أنها مكلفة: 72 بليون دولار سنويّاً في الولايات المتّحدة. وكذلك تكبّد مجتمعنا أثماناً مرتفعة، محليّاً وخارجيّاً. ويشبّه البروفسور يوشاي بنكلر[3]، وهو أستاذ قانون في «جامعة هارفرد»، رقابة «وكالة الأمن القومي» بأمراض اختلال المناعة الذاتيّة التي تتسم بأن الجهاز المنوط به صنع مناعة للجسم ضد الأجسام الغريبة عنه، يصيبه خلل وينفلت ليضرب أنسجة الجسم نفسه، ويصبح ذلك الجهاز مصدراً لأمراضه. والأرجح أنّه تشبيه جيّد.

تشكّل الحريّة الثمن الأغلى للرقابة، وهو خطر حقيقي وماثل إلى حدّ أن أناساً من اتّجاهات أيديولوجيّة متباينة باتوا يعربون عن احتجاجهم على توسّع الرقابة وتدخّلاتها القويّة. وحتى إنّ مجلة محافظة سياسيّاً ومؤيّدة للأعمال، هي **الإيكونومست**، ناقشت في مقال افتتاحي في 2013 بأنّ الرقابة ذهبت بعيداً[4]. وقالت: «وصل الأمر إلى حدّ أن أحد الاعتقادات الراسخة لدى هذه المجلة؛ وهو ضرورة الترحيب بالتقدّم التقني وليس الفزع منه؛ بات في موضع التحدي بمواجهة الحريّة. إذ يجب أن تتضمن الحريّة بعض الحق في الخصوصيّة؛ وإذا كان كل ما نفعله موثق في سجلات متسلسلة، تتقلص الحريّة تماماً».

الإدانة بالمعلومات

في القرن السابع عشر، اشتهر عن السياسي الفرنسي الشهير ريشيليو قوله: «أرني ستة سطور كتبها أشرف رجل في العالم، وأنا كفيل بالعثور فيها على ما يوصله إلى حبل المشنقة». وأعلن لافرينتي بيريا، رئيس الشرطة السرية في عهد جوزيف ستالين في الاتحاد السوفياتي السابق: «أرني الرجل، أريك جريمة». قصد ريشيليو وبيريا المعنى عينه: إذا كان لديك معلومات كافية عن شخص ما، بإمكانك العثور على أدلّة كافية لإدانته بشيء *ما*. وللسبب عينه، يحظر القضاء على الشرطة في بلدان عدّة، أن ينخرط في «حملات تصيّد». وللسبب نفسه وعلى وجه الخصوص، يحظر الكونغرس بصرامة إصدار تفويضات عامة، التي تعني أساساً إعطاء المحقّقين الحق في البحث عن أي شيء[5]. من المستطاع جعل التفويض العام بالغ الأذى، واستعمله البريطانيون إبّان استعمارهم أميركا وسيلة للسيطرة الاجتماعيّة.

تعني الرقابة الشاملة إمكان إدانة كل شخص بتهمة اختراق القانون، بمجرد أن تعقد الشرطة العزم على ذلك. من الخطورة بمكان العيش في عالم تختزن فيه معلومات عن كل ما تفعله، ثم تقدّم دليلاً ضدك في مرحلة لاحقة من حياتك. هناك خطر واضح في السماح للبوليس بأن ينقّب في تلك التراكمات الهائلة من المعلومات، كي يستخرج

منها «دليلاً» على فعل مخالف للقانون، خصوصاً في بلد كالولايات المتّحدة يضم عدّة قوانين عقابيّة وضبابيّة، ما يعطي المدّعين سلطة لإدانة من يريدون وبأي تهمة كانت، مع وجود قوانين فضفاضة بشأن ما يمكن أن يكون دليلاً ماديّاً[6]. ويصح الأمر خصوصاً مع التوسّع في مصطلحات لها وزن قانوني[7]، على غرار جعل «الإرهاب» يشمل الجرائم العادية، و«أسلحة الدمار الشامل» تشمل كل شيء تقريباً بما فيها بنادق الخرطوش. تتسم المصطلحات الأميركية بأنّها فضفاضة إلى حدّ أنّ شخصاً يتبرع بعشرة دولارات للذراع الإنساني في حركة «حماس»، يمكن أن يتهم بالإرهاب[8].

تجعلنا الرقابة في موضع خطورة بأن يساء إلينا من قِبَل الممسكين بالسلطة، حتى لو لم نكن نفعل أي سوء في الوقت الذي وُضِعْنا فيه تحت الرقابة. إنّ تعريف الـ «خطأ» هو شأن اعتباطي، ومن الممكن أن يتغيّر بسرعة. ومثلاً، في حقبة الثلاثينيات من القرن الماضي، كانت الاشتراكية أو الشيوعيّة اتّجاهاً فكريّاً رائجاً، أو على الموضة، في الولايات المتّحدة، ولم يكن المثقفون يعتبرونها خطأ. تغيّر الوضع بصورة دراماتيكيّة في خمسينيات القرن العشرين، مع تولي السيناتور جوزيف ماكارثي إطلاق حملات «مطاردة الساحرات»(*) التي دمّرت الحياة المهنيّة لكثير من المواطنين الأميركيّين المبدئيّين والأذكياء، بالكشف عن تاريخهم السياسي. هل سيُنظر إلى الأشخاص الذين يقرأون الآن مواقع «حركة احتلوا وول ستريت»، أو «حزب الشاي»، أو حقوق الحيوان أو الحق في حمل السلاح، بوصفهم متّهمين بممارسة نشاطات إرهابيّة بعد خمس أو عشر سنوات؟

ويزيد في سوء ذلك الوضع أننا نوّلد كميّات كبيرة من البيانات التي تختزن إلى الأبد. وتستطيع «حملات التصيّد» أن تعود إلى الماضي، وتعثر على أشياء فعلتها قبل 5 أو 10 أو 15 أو 20 سنة، وما زال العدّ مستمراً. يستطيع جيل الكبار حاضراً أن ينجو من تهوّراته في مرحلة المراهقة. لن يمتلك المراهقون حاضراً تلك الميزة؛ لأن حياتهم كلها ستكون موثّقة في سجل أبدي.

(*) إشارة إلى حملات أطلقها متشدّدو الكنيسة الكاثوليكيّة في أوروبا في القرون الوسطى، وأُعدمت فيها نساء كثيرات بدعوى كونهن ساحرات متّصلات بالشيطان.

ثمة ضرر آخر ينجم من الرقابة الحكوميّة يتمثّل في طريقة تصنيف الناس لممارسة التمييز ضدّهم. ويصف البروفسور دانيال سولوف، وهو أستاذ قانون من «جامعة جورج واشنطن»، ذلك الوضع بأنه «كافكاوي»[9].(*) ففي سريّة، يُجمَع معظم تلك البيانات ويستخدم، ولا نملك الحق في دحض تلك الأدلة المستخدمة ضدّنا، بل ولا حتى رؤيتها. ولسوف يزداد الأمر سوءاً عندما تبدأ النُظُم المؤتمتة في تحليل بيانات الرقابة واتّخاذ القرارات المستندة إليها، بصورة أوتوماتيكيّة تماماً.

استُخدِمَت بيانات الرقابة ومعلوماتها في تبرير عدد من العقوبات، بداية من تعريض الناس إلى إجراءات أمنيّة مشدّدة ووصولاً إلى ترحيلهم[10]. في 2012، قبيل انطلاقه لقضاء عطلة في «لوس أنجلوس»، غرّد الشاب الإيرلندي لي فان برايان[11] على «تويتر» قائلاً: «أنا حرّ هذا الأسبوع، كي أنجز بعض النميمة/ التحضير، قبل أن أذهب لتدمير أميركا». كانت الحكومة الأميركيّة ترصد تغريدات «تويتر» كافة[12]. التقط عملاء حكوميّون تلك التغريدة، وقارنوها مع لوائح القادمين إلى أميركا جوّاً، وكانوا بانتظار ذلك الشاب في المطار عند وصوله من إيرلندا. لم تكن كلماته سوى مزاح، لكنه خضع لاستجواب دام 5 ساعات قبل إعادته إلى بلاده[13]. نعرف أن التنكيت في المطارات عن التفجيرات تعرّض صاحبها للاعتقال. وحاضراً، يبدو أنه صار واجباً الحذر عند إصدار وعود ضبابيّة عن مشاكسة دوليّة، في أي مكان على الإنترنت[14].

في 2013، وضع شخص من جزيرة «هايتي» يظهر فيه وهو يتناول مشروباً روحيّاً أثناء قيادة سيارته. اعتقلته الشرطة بسبب تلك الجريمة[15]. ودافع الرجل عن نفسه بالإشارة إلى أن الأمر كان تمثيلاً، والشراب الذي كان يتناوله لم يكن كحوليّاً.

(*) إشارة إلى روايات الكاتب الشهير فرانز كافكا التي تتميّز بأجوائها الكابوسيّة والمأساويّة والعبثيّة، مع إحساس شامل بالضياع الوجودي.

حدثت أمور أشـد سـوءاً في المملكة المتّحدة. إذ سُجِنَ بعض الناس هناك بسبب تغريـدة عنصريّـة[16]، أو تدوينة هاذِرَة على «فيسبوك»[17]. وبالطبع، الأرجح أن الأمر أكثر سوءاً بما لا يقاس في بلدان أخرى اعتادت على سـجن الناس وتعذيبهم بسبب أشياء كتبوها على الإنترنت.

يصـل القلـق إلى أقصاه عند تذكّـر أنّ الجيش الأميركي يوجّه غـارات الـ «درون» استناداً إلى معلوماتـه عمـن يسـتهدفهم القصـف[18]. هنـاك نوعـان مـن التوجيـه للـ «درون»: يسـمّى الأول «القتل الموجّه»، يحدّد فيه الشـخص المستهدف بواسـطة الرقابـة الإلكترونيّة أو سـواها. يطلـق على الثاني تسـمية «القتل بالتوقيـع»[19]؛ نظراً لاستهدافه أشـخاصاً مجهولين يجري تحديدهم وفقاً لسـلوكهم وسـماتهم الشخصيّة، كعمرهـم ونوعهـم الجنسي ظاهريّـاً، وموقعهم جغرافيّـاً، وما يبدو أنهـم منخرطون في فعلـه. عندمـا وصلت غـارات الـ «درون» إلى زروتهـا في باكسـتان عامي 2009 و2010، شـكّل «القتل بالتوقيع» نصف غارات الـ «درون»[20]. لا نملك معلومات عـن مدى دقّة رسـوم الملامح الشـخصيّة («بروفايل») التي اسـتندت تلـك الغارات إليها.

إنّه خطأ كامل. يجب أن نكون أحراراً عند الحديث مع أصدقائنا، أو بثّ رسـالة نصيّة إلى أحد أفراد العائلة، أو قراءة كتاب أو مقال، من دون مكابدة القلق من رأي الحكومة المحتمل في تلك الأمور: سواء الحكومة حاضراً، أو بعد 5 أو 10 سنوات، أو حتى حكومات أخرى. يجب ألا نقلق حيال احتمال فهم أو إساءة فهم أفعالنا، أو أنها ربما تستعمل ضدّنا. يجب ألا نكون عرضة لرقابة من دون حدود[21].

الحجب الحكومي

تعتمـد الحريّة أيضاً على حريّـة تداول الأفكار. ويخنق الحجـب الحكومي المتآزر غالباً مع الرقابة الإلكترونيّة الحريّة والأفكار معاً.

تحمـي الصين مواطنيها من «مخاطـر» الأخبار الأجنبيّة والأفكار الآتية بواسـطة الإنترنـت، بـما مـا يسـمّى «الـدرع الذهبـي» (Golden Shield)، بالأحـرى «جدار النـار الصيني العظيم» (Great China Firewall) [22]، في إشـارة إلى «جدران النار» الإلكترونيّة التي هي برامج لرقابة الحركة على الإنترنت.

واسـتغرق إنجاز ذلك المشروع الضخم 8 سـنوات، بتكلفـة بلغت 700 مليون دولار. وتتمثّـل مهمّتـه في فـرض الحجـب عـلى الإنترنـت. ويشـكل منـع الأفكار المضـرّة وخنق حرية الكـلام أهدافاً ثانويّة لـه[23]، فيما يتمثّل هدفه الرئيس في منع نشـوء منظّمات فعّالة. يعمل ذلك «الجدار الناري» بصورة جيّدة[24]؛ لأن من لديهم تمرّسـاً في التقنيّات الإلكترونيّة يستطيعون تفاديه، لكنه يمنع غالبية الشعب الصيني مـن العثور على أشـياء كثيرة، بداية من المعلومات عـن دالاي لاما، (القائد الروحي لشعب التيبت)، ووصولاً إلى مجموعة من مواقع محرّكات البحث الغربيّة.

ثمة حجـب حكومي يمارس على الإنترنت حاضراً أكثر من أي وقت مضى[25]. ولا يتعلّـق الأمر بالسياسـة وحدهـا. هناك بلدان تحجـب مواقع إلكترونيّة بسـبب طبيعتهـا الجنسـيّة، أو الأفـكار الدينيّـة التي تنشرهـا، أو اسـتضافتها لمنصّات لعب القمار، أو ترويجها لمواد مكيّفة أو نشاطات غير شرعيّة. تعيش غالبية مواطني الشرق الأوسـط تحت حجب حكومي واسع. تحجب فرنسا وألمانيا والنمسا أفكار النازيّين الجـدد[26]، بما فيها المزادات على مقتنيات تعـود إلى الحقبة النازية، فيما تفرض بلدان أخـرى حجباً على المواقع التي تحرّض على العنف. ويمنع «التشريع 72» الفيتناميّين مـن نقـاش أمور عامة عـلى الإنترنت[27]. وتحجـب بلدان كثيرة المحتـوى المخالف لقوانـين الملكيـة الفكريـة[28]. ويعدُّ حجـب المواقع الإباحيّة جنسـيّاً أمـراً بديهيّاً في بريطانيـا، عـلى الرغم من وجود خيار بالخروج من ذلـك الحجب[29]. وفي 2010، حجبت الولايات المتّحدة موقع «ويكيليكس»[30].

يحظى معظم الحجب بدعم من الرقابة، ما يؤدّي إلى فرض حجب ذاتي. إذا علم الناس أن الحكومة تراقب كل ما يقولونه، يصبحون أقل ميلاً لقراءة مواضيع محظورة أو حتى الحديث عنها. شكّل ذلك هدفاً لقانون أصدرته روسيا في 2014، يطلب من أصحاب المُدوّنات الإلكترونيّة «بلوغرز» (Bloggers) التسجيل لدى الحكومة[31]. ويفسّر ذلك أيضاً سبب نجاح «جدار النار الصيني العظيم» كأداة للحجب؛ إذ لا يعود ذلك إلى القدرات التقنيّة لذلك الجدار وحدها، بل أيضاً إلى الخطر الذي يتهدّد من يحاول تفاديه، بأن مواطنين آخرين للحكومة ربما اكتشفوه وأبلغوا عنه. لا يعني ذلك أنّ أولئك المُبَلّغين هم بالضرورة متوافقون مع الحكومة[32]، بل إنهم يخشون أن يعاقَبوا إن هم لم يبلغوها عن المخالفين. وفي الصين، تفرض شركات الإنترنت حجباً على مستخدميها يفوق المطلوب منها رسميّاً[33].

وكلما زادت العقوبات على من يُضبط متهرباً من رقابة الحكومة، زاد الميل إلى ممارسة الحجب الذاتي[34].

تأثيرات مفزعة

تملك الرقابة تأثيرات مفزعة في المجتمع[35]. لاحظت ذلك سونيا سوتومايور، القاضية في «المحكمة الأميركيّة العليا»، أثناء إبدائها رأيها في قضية رفعت في العام 2012، بشأن دسّ الـ «إف بي آي» جهازاً للتتبع متّصل بالـ «جي بي إس» في سيارة أحد الأفراد. إذ قالت سوتومايور: «يؤدي التنبّه إلى احتمال وجود رقابة حكوميّة، إلى إثارة فزع بشأن حريّتي التعبير والترابط. لكن القدرة غير المحدودة للحكومة في جمع معلومات تكشف مناحيَ خصوصيّة عند الأفراد، هي عرضة لإساءة الاستخدام. وتكون المحصلة النهائية أن التتبّع بالـ «جي بي إس» يوفّر بتكلفة بسيطة كميات أساسيّة من المعلومات عن كل شخص ترغب الحكومة في تتبعه[36]، مع غياب الضوابط المناسبة؛ ولربما أثّر ذلك في علاقة المواطن مع الحكومة بطريقة لا تتلاءم مع المجتمع الديمقراطي».

كتب البروفسور إيبين موغلن، وهو أستاذ قانون في «جامعة كولومبيا»، عن مسألة الرقابة، لافتاً إلى «أنّ الحضور الشامل للتنصّت المتعدي، هو أمر يخلق الخوف الذي هو العدو للحريّة المنظّمة العاقلة»[37].

في الولايات المتّحدة، بدأنا في رؤية بواكير ذلك الفزع. ووفق تقرير لمنظّمة «هيومن رايتس ووتش»، أعاقت الرقابة الحكوميّة كتابة الصحافيّين عن مجتمع الاستخبارات، الأمن القومي، وقوى إنفاذ القانون، إذ باتت المصادر أقل ميلاً للاتّصال بهم، بل صاروا هم أنفسهم يخشون الملاحقة والإدانة[38]. واستنتجت «هيومن رايتس ووتش» أن هناك قصصاً تقضي المصلحة الوطنيّة بالكتابة عنها، لكن لم يجر تناولها إعلاميّاً، ما يعني أن الجمهور أصبح على درجة أقل من الدراية والمعرفة. ذلك هو بالضبط الأثر المفزع الذي تولّده الرقابة.

وتأثّر بالأمر عينه المحامون الذين يعملون على قضايا لها صلة ما بالاستخبارات[39]، كالإرهاب والمخدّرات ووكلاء الحكومات الأجنبيّة. وعلى غرار الصحافيّين، بات المحامون يخشون أن تراقب محادثاتهم، وأنّ تصل حواراتهم مع موكّليهم إلى أيدي الادّعاء[40].

عقب 9/ 11، أوصلت الرقابة الكتّاب إلى فرض حجب ذاتي على أنفسهم[41]. إذ تجنّبوا الكتابة عن موضوعات معيّنة وإجراء تحقيقات بشأنها، وصاروا حذرين عند الاتّصال مع المصادر والزملاء، بل حتى أصدقائهم في الخارج. وأظهر استطلاع أجراه «مركز بيو للبحوث» عقب نشر الوثائق الأولى لسنودن، أنّ الناس لم يعودوا راغبين بالحديث عن «وكالة الأمن القومي» على الإنترنت[42]. وكذلك بيّن استطلاع أكثر توسّعاً أجراه «مركز هاريس» أن نصف الأميركيّين غيّروا موضوعات البحث والقراءة والمحادثة بواسطة الإنترنت؛ بسبب رقابة «وكالة الأمن القومي»[43]. أدّت الرقابة إلى فزعٍ من استخدام الإنترنت لدى المسلمين الأميركيّين[44]، ومجموعات البيئة[45]، ومناصري الحق في حمل السلاح، ومن ينشطون بشأن سياسات مكافحة

المخدّرات، والعاملين في مجال حقوق الإنسان. وعقب كشوفات سنودن في 2013، صار الأفراد في أنحاء العالم أقل ميلاً لوضع تعابير شخصيّة حساسة على محرّك البحث «غوغل»[46].

في 2014، لاحظ تقرير «المفوضيّة العليا لحقوق الإنسان في الأمم المتّحدة» أنّ «مجرد التلويح باحتمال أن تلتقط بيانات الاتّصالات، يؤدّي إلى الإخلال بالخصوصيّة، مع إمكان حدوث تأثيرات مفزعة في الحقوق، وضمنها الحق في التعبير وتكوين الروابط»[47].

لا يتعلّق الأمر بعقدة اضطهاد مرضيّة وهذيان البارانويا. في إحدى حملاته الانتخابيّة في 2012، أشار الرئيس الفرنسي نيكولا ساركوزي إلى أنّ «كل شخص يتردّد بانتظام على مواقع شبكيّة منحازة للإرهاب أو تنشر الكراهية، سوف يحكم عليه بالسجن»[48].

لا يقتصر الخوف من التمحيص على أفعال الحاضر وحدها؛ بل تشمل الماضي أيضاً. إذ بات السياسيّون يعيشون في عالم تلاحقهم فيه كاميرات المعارضة باستمرار، على أمل تسجيل ما يمكن وضعه خارج السياق. وتحاكم في الحاضر كل الأشياء التي قالوها في الماضي، وبدقّة أكبر مما كان متخيّلاً قبل سنوات قليلة. تخيّل لو أن الأمر عينه ينطبق على كل من يسعى إلى وظيفة ما.

بالطبع، لا يتأثّر الناس بالرقابة بشكل متساوٍ. لا يعير بعضنا بالاً للرقابة الحكوميّة، ولا يتأثّر بها كليّاً. في المقابل، يتأثّر بعضنا كثيراً، خصوصاً من ينتمون إلى مجموعات دينيّة، واجتماعيّة، وإثنيّة واقتصاديّة لا تروق للنخبة الحاكمة.

تتمحور الملاحظة الرئيسة للكاتب جيرمي بنثام بخصوص الـ «اوبتِكون» (راجع الفصل 7)، حول فكرة أن الناس يصبحون مطواعين وموالين عندما يعتقدون بأنّهم مراقبون. يشكّل الـ «اوبتِكون» هندسة للسيطرة الاجتماعيّة. فكّر في طريقة تصرّفك عندما تسير سيّارة بوليس بمحاذاة سيارتك، أو في حال بلد برمّته حين

يتـولّى موظّفو الحكومة التنصّت عـلى مكالماتهم[49]. عندما نعرف أن كل شيء يجري تسـجيله، نغـدو أقل ميلاً للحديـث بصراحة والتصرف إفراديّـاً. عندما نكون تحت تهديـد دائـم بالمحاكمة والنقد والعقاب على تصرّفاتنا، ينتابنا خوف من أنه، إما الآن أو في مسـتقبل غير محدّد، سوف تسـتحضر البيانات التي خلّفناها وراءنا، كي تديننا بواسـطة أي شيء تركـز عليه الحكومة يومئذٍ من التصرفـات التي عددناها ذات مرّة بريئة وخصوصيّة. وكردّة فعل، لا نفعل شيئاً خارج المألوف. نفقد خصوصيّتنا، فيما تركد حركيّة المجتمع. لا نسـائل السـلطة ولا نتحداها. نغدو مطيعين ومستسلمين. نصبح أقل حريّة.

منع التمرّد والتغيّر الاجتماعي

تملك تلك التأثيرات المثيرة للفزع وقعاً مدمّراً في الخطاب السياسي بوجه خاص. هناك قيمة للتمرّد[50]. وربما امتلك خرق القانون بعض القيمة أيضاً، مهما بدا القول غريباً. ويعمل التمرّد وخرق القانون على تحسين المجتمع. إنّ الرقابة الشاملة الكلية القدرة هي العدو للديمقراطيّة، والحريّة، والتقدّم والتحرّر.

يتطلّب الدفاع عن ذلك التأكيد دفاعاً قويّاً ومرهفاً– هو ما فعلته في كتابي السابق كَذَبَـة ومتمرّدون[51]– لكنه يمتلك أهمية حيويّة للمجتمع. لنفكر بالأمر على النحو التـالي: بالولايات المتحدة، ثمة ولايات صارت على شـفا تغيير قوانين راسـخة منذ عقود بصدد العلاقات المثليّة جنسيّاً وكذلك استخدام الماريجوانا (حشيشة الكيف). لـو أن الرقابـة عضّـدت القوانـين القديمة لمـا تغيّـرت، ومـا كنا لنصـل إلى حدّ أن معظـم المواطنين باتوا يقبلون تلك الأمور. لا بد أن توجد مرحلة تكون فيها الأمور غـير شرعيّة لكـن يجري تقبّلها باطّـراد، ما يدفع النـاس إلى التلفّـت حولهم قائلين: «أتعرف؟ إنّها ليست سيّئة تماماً». صحيح أن تلك العملية تستغرق عقوداً، لكنها لا توجد أصلاً من دون اختراق القوانين. وصرّح الموسـيقار والمفكّر الأميركي فرانك

زابا بشيء مماثل في 1971، قائلاً: «دون الخروج عن العرف السائد، يضحي التقدّم مستحيلاً»[52].

يؤدّي الإنفاذ الكامل للقوانين بمساعدة الرقابة إلى شلل في تلك العملية. نحن بحاجة إلى أمن منقوص[53]، بمعنى وجود نُظُم تترك الحرية للناس كي يجرّبوا أشياء جديدة، بطريقة تشبه ما تحدثه جلسات العصف الفكري غير الموثّقة، من تليين للكوابح وتدعيم للابتكار. دون ذلك، يصبح مستحيلاً التدرج من وضع تكون فيه أشياء غير شرعية ومرفوضة، إلى وضع تغدو فيه شرعيّة لكن مع شيء عدم التيقن بشأن رفضها، إلى الاستمرار في كونها غير شرعية لكنها مقبولة على الأرجح، ثم الانتهاء إلى جعلها شرعيّة.

من المهم ملاحظة ذلك الأمر. هناك حريّات ننعم بها حاضراً لكنها كانت في زمن ماضٍ تعتبر مهدّدة أو حتى جرميّة، بعيون السلطة الحاكمة آنذاك. ما كانت تلك التغييرات لتحدث أبداً لو أن السلطات امتلكت القدرة على تحقيق السيطرة الاجتماعيّة بالرقابة.

يشكّل ذلك أحد الأسباب الرئيسة كي نهتم جميعاً بشأن التركيبة الصاعدة حاضراً للرقابة، حتى لو لم تصبنا آثارها المفزعة بصور شخصية. إذ نعاني تلك الآثار لأن الناس حولنا يصبحون أقل قدرة على تبني أفكار سياسية أو اجتماعيّة جديدة، أو التصرّف بطرق غير مألوفة. لو نجحت رقابة السيناتور المتشدّد جوزيف مكارثي في إخراس صوت داعية الحقوق المدنيّة الأفريقي- الأميركي القس مارتن لوثر كينغ، لترك الأمر آثاراً تطال ما هو أبعد من كينغ وأسرته.

بديهي القول إن ثمة أشياء غير شرعيّة ستبقى غير شرعية للأبد: كالقتل والسرقة وما إلى ذلك. في المقابل، يولّد التطرّف في دقة إنفاذ القانون، تداعيات غير مسبوقة. ماذا يعني للمجتمع أن تكون الشرطة قادرة على متابعة سيارتك على مدار الساعة، وإرسال فواتير لك في آخر الشهر تتضمن كل مرّة زدت فيها من سرعتك، أو

تجاوزت إشارة حمراء، أو انعطفت إلى اليسار بالخطأ، أو لحقت بالسيارة التي أمامك مـن مسـافة قريبة جداً؟ مـاذا يعنـي أن تكون السـلطة المحليّة في بلدتـك قادرة على اسـتعمال الصور الجويّة بطريقة أوتوماتيكيّة[54]، لتوقع عليك غرامة كلما تأخّرت في جزّ عشـب حديقتك، أو ربما لم تنتظم في مشيتك؟ يستند نظامنا القانوني على محاكمة الأمور إنسـانيّاً. وفيما تحيق المخاطر بالأحكام المسـبقة والمنحـازة، فهناك مخاطر أكبر من إبدال تلك الأحكام بمحض جداول خوارزميّة تعمل بكفاءة[55].

ثمة احتمال بأن تقود الرقابة الشاملة إلى مجتمع من النوع الذي رسمه فيلم «تقرير الأقليّـة» (ظهر في 2002، مـن بطولة الممثل توم كروز)، بمعنـى أن يضحي الناس عرضة للخضوع إلى تحقيق بوليسي قبل إتيانهم بأي جرم[56]. وفعليّاً، بدأت وكالات إنفاذ القانون في اسـتخدام أدوات تحليليّة استباقيّة للتعرّف إلى المشتبه فيهم، وكذلك لتوجيـه التحقيقـات[57]. ولم تعد سـوى خطوات قصيرة تفصلهـا عن الوصول إلى مجتمع «الأخ الكبير» وجرائم الفكر.

إنّ مفهـوم جعل الإفلات من جرائم معيّنة أمراً مسـتحيلاً، هـو جديد[58]- مع احتـمال كونه ناجماً عن تلك التقنيّات المتقدّمـة كلها- ويجدر التفكير فيه بحذر وتروٍّ قبـل وضعـه موضع التنفيذ. ووفق تعبير البروفسـور يوشـاي بِنكلـر: «النقص عن الكمال هو بُعدٌ أساسي في الحريّة»[59].

زحف السريّة

تتمرّد السريّة عموماً على الرقابة الحكوميّة، وكذلك تمثّل خطراً على المجتمع الحر والمفتوح.

في الولايـات المتّحـدة، عبّر ذلك عن نفسـه بصور متنوّعة، إذ وسّـعت الحكومة تعريـف ما يمكن اعتبـاره سراً. تتمثّل إحدى حقائق الأمـن القومي في كون السريّة ضروريّـة في شـؤون الاسـتخبارات والدفاع والسياسـة الخارجية[60]. إذا كشـفت

الحكومة أشياء معيّنة- كتحرّكات الفرق العسكرية، وقدرات الأسلحة والمواقف الفعليّة في المفاوضات- يتمكن العدو من تغيير تحرّكاته بما يخدم مصلحته. استمرت صحة ذلك المفهوم للسريّة العسكريّة طيلة آلاف السنوات[61]، لكنه تغيّر حاضراً بشكل دراماتيكي[62]. أنا أستعمل الولايات المتّحدة كنموذج عن ذلك. في الحرب العالمية الأولى، كُنّا منشغلين بسريّة وقائع محدّدة، كمواقع الوحدات العسكريّة والخطط التفصيليّة للمعارك. في الحرب العالمية الثانية، جرى توسيع مفهوم السريّة ليشمل عمليات واسعة النطاق ومساحات كاملة من المعرفة، كليهما معاً[63]. إذ لم يقتصر الأمر على سريّة برنامجنا لبناء قنبلة ذريّة، بل إن كامل الحقول العلميّة المتعلقة بالسلاح النووي عُدت سريّة أيضاً[64]. عقب 9/ 11، عمّمنا المفهوم كثيراً[65]. وحاضراً من المستطاع وصف أي شيء تقريباً بأنه سرّ.

وبالنتيجة، تفجّرت سريّة الحكومة الأميركيّة. لا أحد يعرف الرقم الدقيق[66]- لأنه سرّ بالطبع- لكن التقديرات تشير إلى أن بلايين الصفحات من الوثائق الحكوميّة الأميركيّة، توضع في خانة السريّة سنويّاً. في الوقت عينه، تكاثرت كالفطر أعداد الأشخاص الممنوحين أُذونات أمنيّة. وفي تشرين أول/ أكتوبر 2012، حاز قرابة 5 ملايين شخص في الولايات المتّحدة أُذونات أمنيّة[67] (من بينهم 1.4 مليون مصنفون في خانة «سري جداً»)، ويساوي ذلك زيادة بـ50 ٪ عما كانه في 1999.

توضع في خانة السريّة تفاصيل الرقابة كافة التي تمارسها «وكالة الأمن القومي» خشية أن تتسرّب إلى الأشرار[68]. (سأعود إلى تلك المحاججة في الفصل 13). قبل كشوفات سنودن، لم يكن متاحاً قراءة التوجيهات السياسيّة الرئاسيّة التي خولت لـ«وكالة الأمن القومي» معظم أعمالها في الرقابة. لم يكن مسموحاً حتى بقراءة أوامر المحكمة التي تتخصّص بتخويل أعمال تلك الرقابة[69]. كانت تلك الأمور سريّة كلها، وكانت لتبقى كذلك لولا أن كشوفات سنودن أدّت إلى رفع غطاء السريّة الحكوميّة عن حفنة منها.

لا تقتصر زيادة مستويات السريّة على الجيش و«وكالة الأمن القومي» وحدهما. إذ شرعت قوى إنفاذ القوى القانون محلياً في تلفيع مراقباتها الخاصة برداء السريّة. ومثلاً، صار طلب الشرطة رقابة هاتف خلوي ما أمراً روتينياً، تصادق عليها المحاكم التي تخوّله تلك السلطة[70]. (لا تعترف الشرطة في المملكة المتّحدة ولو بمجرد أنّها تستخدم تلك التقنية)[71]. وهناك أمثلة كثيرة عن ذلك.

توهن تلك السريّة الضوابط والكوابح الموضوعة للإشراف على الرقابة، وكذلك، بصورة أوسع، التثبت من كوننا نعامل جميعاً بعدالة من قِبَل قوانيننا. منذ هجمات الإرهاب في 9/ 11، صارت الرسائل الأمنيّة للـ «إف بي آي» و«وكالة الأمن القومي»، تأتي مرفقة بحظر قضائي. إذ يُمنع من يتلقى تلك الرسائل من الحديث عنها، حتى بتعابير عموميّة[72]. ويصعّب ذلك أمر مقارعة تلك الرسائل في المحاكم.

تختبئ الحكومات أيضاً خلف اتفاقيّات مع الشركات بعدم التصريح. وتستند الـ «إف بي آي» وقوات الشرطة المحلية على تلك الاتفاقيّات في عدم الإفصاح عن طريقة عمل نظام «ستنغراي» (راجع الفصل الخامس) في رقابة الهواتف الخلوية[73]. وتلجأ قوات الشرطة المحليّة إلى الممارسة عينها في رفضها كشف تفاصيل الجداول الخوارزميّة المستخدمة في أدوات التحليل الاستباقيّة، التي تستخدم في تدخّلات ضباط الشرطة[74].

عبّرت سريّة الحكومة عن نفسها بطريقة ثانية، وهي كونها دُفِعَت إلى درجة قصوى. تملك الولايات المتّحدة إطاراً قانونيّاً معقّداً في التصنيف، لكن يجري تجاهله باطّراد[75]. وتسيء السلطة التنفيذيّة استعمال الصلاحيات التي تحوزها لإبقاء المعلومات العامة بعيدة عن أعين العموم[76]. تنأى السلطة التنفيذيّة بأسرارها عن الكونغرس[77]. وتحتفظ «وكالة الأمن القومي» بأسرارها بعيدة عمن يناط بهم مهمة الإشراف على الوكالة[78]، بما في ذلك الكونغرس[79]. يكتم بعض

أعضاء الكونغرس أسراراً عن بقية أعضاء الكونغرس[80]. وتحتفظ المحاكم السريّة بأسرارها لنفسها[81]، وحتى «المحكمة العليا» صارت أكثر ميلاً لإبقاء وثائقها طيّ السريّة[82]. في واشنطن، تعدُّ المعرفة نقوداً، ويعمد مجتمع الاستخبارات إلى مراكمتها.

تأتي العلامة الثالثة على سريّة الحكومة من واقع أنها تعاملت بقسوة تامة مع أولئك الذين كشفوا أسرارها: لنسمّيهم «مُطلِقو صافرات الإنذار». أبدى الرئيس باراك أوباما حماسة خاصة في محاكمة الأفراد الذين كشفوا الأعمال الخاطئة للوكالات الحكوميّة[83]. ومنذ انتخابه في العام 2008، أصر على محاكمة ثمانية أشخاص بسبب كشفهم معلومات سريّة إلى الصحافة. كان الرقم عينه هو ثلاثة أشخاص منذ إقرار «قانون التجسّس» في العام 1917 [84].

في القانون الأميركي، لا يعدّ إطلاق صافرة إنذار لتنبيه الجمهور عذراً مقبولاً في ما يتعلّق بالاستخبارات؛ إذ يمنع «قانون التجسّس» الشخص المُدّعى عليه من شرح سبب تسريبه معلومات سريّة. كان دانيال إلسبرغ هو أول من حوكم تحت ذلك القانون في العام 1971، ومُنع من تفسير أعماله أمام المحكمة. وعندما حوكم توماس درايك، وهو مدير تنفيذي سابق في «وكالة الأمن القومي»، مُنع من استخدام تعبيري «إطلاق صافرة إنذار» و«الإفراط في السريّة» أثناء محاكمته[85]. وكذلك مُنِعَت تشيلساماننغ(*) من استخدام دفاع مماثل أثناء محاكمتها[86].

ادّعى إدوارد سنودن أنّه من مُطلِقي صافرات الإنذار[87]. ويوافق كثيرون، وأنا منهم، على ذلك الزعم، فيما يرفضه آخرون. وأصرّ وزير الخارجية جون كيري على وجوب «أن يعود سنودن إلى بلاده، ويقف أمام نظامنا القضائي، ويدافع عن قضيته»[88]. وكذلك زعمت وزيرة الخارجيّة السابقة هيلاري كلينتون أنّه «إذا أراد

(*) حوكمت في قضية "ويكيليكس" لأنها سّربت وثائق سريّة عندما "كانت" جندياً يعمل في المعلوماتيّة اسمه برادلي ماننغ الذي طلب تغيير جنسه في خضم محاكمته، وتحوّل إلى الأنثى تشيلسا.

سنودن أن يعود مع علمه أنّه يتحمل مسؤولية أفعاله ويستطيع الدفاع عن نفسه، سيجب عليه اتّخاذ ذلك القرار بنفسه»[89]. يقدّم التصريحان كلاهما نموذجاً عن نفث دخان التضليل السياسي[90]. إذ لا يتيح القانون الساري حاضراً لسنودن أن يدافع عن نفسه.

وبقدر ما تتطلّبه الرقابة الحكوميّة من سريّة، يفقد الناس سلطة النقاش والتصويت على ما تفعله حكومتهم باسمهم، أو الإفصاح إلى من ينتخبونهم عما يفكرون أنه يجب القيام به. من السهل نسيان، في خضم السيل الطامي من العناوين الإعلاميّة عن «وكالة الأمن القومي» وبرامجها في الرقابة، أن أحداً ما كان ليعلم شيئاً عنها، لولا أن سنودن كشف ما كانت تفعله الوكالة، متحمّلاً أكلافاً ومجازفات شخصيّة كبرى.

إساءة استعمال

في وقت مبكّر من العام 2014، استهل شخص ما حساباً تهكّمياً على «تويتر»، مستخدماً اسم جيم آرديس، عمدة بلدة «بيوريا» بولاية «إلينويز». كان تهكّماً مؤذياً إلى حدّ كبير، ما أثار حفيظة آرديس. وأدى غضبه إلى إطلاق سلسلة من الحوادث، تضمّنت حصول الشرطة المحلية بطريقة غير مشروعة على أمر قضائي يفرض على «تويتر» تسليم معلوماته عن شخصية ذلك الشخص[91]، ثم أغارت الشرطة على بيته، واعتقل جون دانيال. لم تُسَق تهم ضد دانيال، أساساً لأن الأخير لم يقم بأعمال غير قانونيّة. وحاضراً، يتابع «الاتحاد الأميركي للحريّات المدنيّة» دعوى قضائيّة ضد بلدة «بيوريا» لمصلحة دانيال.

إنّ نظم الرقابة كلها عرضة لإساءة الاستعمال. في السنوات الأخيرة، استعملت الشرطة الرقابة لاستفزاز المعارضة، وكذلك للتحرّش بأناس ترغب في مضايقتهم، كما كان الحال مع دانيال. هناك مثل عن ذلك حدث في 2014؛ إذ اعتادت الشرطة في «نيو جيرسي» روتينيّاً أن تلتقط صوراً للمحتجين في المناسبات التي يستضيفها

حاكم الولاية كريس كريستي، إلى أن أصدر مدّعي عام الولاية أمراً قانونيّاً يوقف تلك الممارسة[92]. وفي العام 2014 أيضاً، بتنا نعرف أن الـ «سي آي إيه» اخترقت أجهزة كومبيوتر يملكها موظفون في «لجنة الاستخبارات في مجلس الشيوخ» التي كانت تدقّق في أعمال الـ «سي آي إيه». وصرنا نعرف أنّه في 2013، تجسّست «وكالة الأمن القومي» على اتّصالات الأمم المتّحدة، مخترقة بذلك القانون الدولي[93]. نعرف أن إساءة استعمال من الأنواع كافة حدثت من قِبَل سلطات الرقابة المحليّة في الولايات، وعلى المستوى القومي أيضاً.

تحدث أصناف من إساءة الاستعمال داخل منظّمات الرقابة نفسها أيضاً. ومثلاً، درج موظّفو «وكالة الأمن القومي» على التنصّت على المكالمات الهاتفية الشخصيّة للأميركيّين في دول أجنبيّة، واعتراض رسائل الـ «إيميل»، كما تداولوا الصور ذات الإيحاءات الجنسيّة الفوّارة بين مكاتبهم. جاءت تلك المعلومات من شخصين كانا يعملان في اعتراض البريد الإلكتروني في 2008 [94]، ومرّة أخرى من سنودن في 2014[95]. ونعرف من وثائق «وكالة الأمن القومي» أنّ عملاءها تجسّسوا أحياناً على أشخاص يعرفونهم في الولايات المتّحدة، وكانوا يسمّون تلك الممارسة «لوف إنت» (LOVEINT) [96]. وتلاحظ وثائق التدقيق في أعمال الوكالة أنها اخترقت بنفسها قواعد عملها في 2276 مرّة خلال 12 شهراً، بين عامي 2011 و2012 [97]. إنّه رقم مرتفع- ثمانية اختراقات يوميّاً- لكن الرقم الحقيقي ربما كان أكبر بكثير[98]. وبأثر من الطريقة التي تراقب فيها الوكالة عملها، تستطيع الوكالة أن تحدّد عدد الاختراقات التي تستطيع اكتشافها.

ليست تلك بمشكلة جديدة، ولا تقتصر على «وكالة الأمن القومي». إذ يُظهر التاريخ الأميركي الحديث وجود مراحل من الإساءة المنهجة لاستعمال الرقابة: ضد قادة العمال ومن المشتبه فيهم بأنهم شيوعيّون، في مرحلة ما بعد الحرب العالمية

الأولى؛ وضد قادة حركة الحقوق المدنيّة(*) والمحتجّين على الحرب في فيتنام. ليست التفاصيل المحدّدة عن تلك المراحل بجذّابة، لكن يمكن الحديث عن اثنين منها.

- بفضل الرقابة المكثّفة، عرف السيناتور ج. إدغار مكارثي بوجود علاقات عاطفيّة للقس الأفريقي- الأميركي مارتن لوثر كينغ خارج رباط الزوجيّة، وخطّ رسالة مُغفَلَة المُرْسِل محاولاً دفعه إلى الانتحار في العام 1964 [99]، إذ ورد فيها: «كينغ. انظر إلى قلبك. تعلم أنك فاسد كليّاً وتمثّل إساءة لنا نحن الزنوج جميعاً. يحصل البيض في هذه البلاد على ما يكفيهم من الفساد، لكني واثق بأنهم لا يملكون شخصاً بمثل فسادك. أنت لست رجل دين، وتعرف ذلك جيّداً. أكرّر أنّك فاسد عظيم، بل شيطان وشرير. أنت لا تستطيع أن تؤمن بالله... من الواضح أنك لا تؤمن بأي مبدأ أخلاقي شخصي... كينغ: هنالك شيء وحيد تبقى لك كي تفعله. أنت تعرفه جيداً. بقي لديك 34 يوماً لتفعل ذلك. (جرى اختيار الرقم لسبب محدّد، هو أنّ له دلالة عمليّة). أنت انتهيت. لم يتبق لك سوى طريق وحيد للخلاص. من الأفضل لك اعتماد ذلك الخيار، قبل أن تتعرّى نفسك الفاسدة وغير الطبيعيّة أمام الأمّة».
- في ما يلي الكلمات التي استعملها الكونغرس في وصفه لبرنامج «كوينتلبرو» الذي استخدمته الـ «إف بي آي» في الرقابة عام 1976 [100]: «فيما تمثّل الهدف المُعلَن من تلك البرامج في حماية «الأمن القومي» أو منع العنف، يقرّ الـ «إف بي آي» بأنّ معظم أهدافها كانوا أشخاصاً مسالمين غير عنيفين، ولم تكن لهم صلة بقوة أجنبيّة. بالطبع، جرى استهداف أشخاص ومنظّمات سلميّة من قِبَل الـ «إف بي آي»؛ لأنها حسبت أن لديهم ميلاً «كامناً» للعنف؛ وأما المواطنون غير العنيفين الذين عارضوا الحرب في فيتنام، فاستهدفتهم الـ «إف بي آي» لأنهم يقدّمون «الدعم والأمان» للمتظاهرين العنيفين، بإعطاء الاحترام لقضيّتهم... لكن برنامج «كوينتلبرو» لم يكتف ببساطة بمجرد اختراق الدستور والقانون. ففي سياق برنامج

(*) أطلِقَت تلك التسمية على حركة سلمية نادت بالمساواة في الحقوق بين السود والبيض، في ستينيات القرن العشرين، وكان القس الإفريقي- الأميركي مارتن لوثر كينغ أبرز قادتها.

«كوينتلبرو»، وضعت الـ «إف بي آي» يدها على القانون، وذهبت إلى أبعد من جمع المعلومات، وتخطّت المهمة الموكلة لها بدعم إنفاذ القانون؛ فعملت خارج العملية القانونيّة برمّتها؛ وعلمت سراً على إقلاق مواطنين ومجموعات ومضايقتهم وضرب مصداقيتهم».

لم يتغيّر شيء. وبعد 9/ 11 تجسّست الولايات المتّحدة على «حركة احتلوا وول ستريت»[101]، ونشطاء الدفاع عن الحق في الإجهاض ورافضيه أيضاً[102]، ونشطاء السلام[103]، ومحتجّين سياسيّين آخرين[104].

- تجسّس الـ «إف بي آي» و«وكالة الأمن القومي» على أميركيّين مسلمين بارزين لا صلة لهم مع الإرهاب[105]، ومن ضمنهم: فيصل جيل (نشط لأوقات طويلة في صفوف الحزب الجمهوري، وترشّح لمنصب عام، وكان لديهم تفويض أمني مرتفع المستوى)، وعاصم غفور (وهو محامٍ بارز تولى تمثيل أشخاص في قضايا متّصلة بالإرهاب)، وهوشانك أمير أحمدي (بروفسور في العلاقات الدوليّة من «جامعة روتغرز»)، ونهاد عوض (المدير التنفيذي لأكبر منظّمة للدفاع عن حقوق الأميركيّين- المسلمين في الولايات المتّحدة).
- تحت غطاء السريّة، تسلّل بوليس نيويورك إلى أحياء الأقليّات[106]. وراقب مساجد، واخترق مجموعات طلابيّة وسياسيّة، وتجسّس على شرائح مجتمعيّة بأسرها. وكرّة أخرى، استُهدِف أميركيّون بسبب انتمائهم إلى هويّة إثنيّة محدّدة، وليس لإدانتهم بجرائم ولا بأفعال خارجة عن القانون. نفّذ كثيرٌ من تلك العمليات بمعونة من الـ «سي آي إيه» على الرغم من أن القانون يحظر عليها التجسّس على أميركيّين.

هنالـك المزيـد مـن تلـك الشـواهد، إذ تجسّـس «مركـز الانصهار» في بوسـطن على «ناشـطين مـن أجل السـلام»[107]، والمنظّمة النسـويّة المناهضـة للحرب «كود بينـك» (Code Pink) وحركـة «احتلـوا وول سـتريت». في 2013، تعاونت مدينة بوسـطن مع شركة «آي بي أم» في نشر مجموعة من كاميرات الفيديو لرقابة مهرجان موسـيقي[108]. في تلك الفترة عينها، تجسّست وحدة «النشاط على الأرض لمكافحة التجسـس» التابعـة للبنتاغون على مجموعة من الأميركيّـين الأبرياء، وهو أمر يحظره القانون على وزارة الدفاع الأميركيّة[109].

وفي عمل يذكّر بمحاولة هوفر اسـتفزاز القسّ مارتن لوثر كينغ، عملت «وكالة الأمـن القومـي» عـلى تتبع أنـماط مشـاهدة أشرطة الجنـس الإباحي لـدى مجموعة مـن الأميركيّـين- المسـلمين، ممـن يعملون عـلى «تحويل» النـاس باتّجاه تبنـي أفكار متطرّفـة[110]، وهؤلاء ليسـوا إرهابيّـين، لكنهم يسـتخدمون خطاباً سياسـيّاً لدفع الآخرين صوب التطرّف. وكانت الفكرة من تلك الرقابة هي ابتزاز تلك المجموعة.

في 2010، فتّشـت «وكالـة مكافحـة المخـدرات» محتويـات الخلـوي لامـرأة مـن مقاطعـة «آلبينـي»، بعـد الحصـول عـلى إذن قانـوني. لكـن الوكالـة احتفظت بالصـور الحميمـة التي عثرت عليها كـي تصنع صفحة مزيّفة باسـم تلك المرأة على «فيسـبوك»[111]. وعندما مثلت الوكالة أمام القضاء، توسّـعت الوكالة في استخدام حجـة مفادهـا أن موافقـة تلك المرأة عـلى تفتيش هاتفهـا يحمل موافقـة ضمنيّة على الاستيلاء على هويّتها.

وتسيء السـلطات المحليّة أيضاً اسـتخدام قـدرات الرقابـة. في 2009، أعارت «مدرسـة مقاطعة ماريون السـفلى» مجموعة من أجهزة الـ «لاب توب» إلى طلبة في المرحلة الثانويّة العليا، بهدف مسـاعدتهم في إنجاز فروضهم. وزرع مدراء المدرسـة برامج تجسّـس في تلك الحواسـيب[112]، فسـجّلت دردشـات التلامذة مع بعضهم بعضـاً، ورصـدت مواقع الإنترنت التـي زاروها، بل إنها- ولعل تلـك أكثرها إثارة

للتقـزز- صوّرتهـم خلسـة في غرف نومهم. وبـرزت تلك القضيـة إلى العلن عندما واجه مسـاعد مدير المدرسـة الطالب بلايك روبنز بصور تظهره وهو يتعاطى حبوباً مهلوسّـة متخفيّـة بهيئـة حبوب للحلـوى. وبالتدقيـق، تبيّن أنها حلـوى من نوعين شهيرين في أميركا، وأدينت المدرسة بسبب تلك الممارسات الاعتدائيّة المسيئة.

إضافة إلى إساءة استخدام السلطة بشكل واضح، هناك التوسّع الحتمي للسلطة الذي يرافق كل نظام بيروقراطي واسـع وقوي. ويشـار إلى ذلك بمصطلح «زحف المهمـة». ومثلاً، بعـد 9/ 11، تآزرت جهود الـ «سي آي إيه» مـع وزارة الخزانة، في جمع بيانات عن معاملات ماليّة لأميركيّين؛ سـعياً لتقصي التمويل المحتمل لجماعات إرهابيّـة مسـتقبلاً. وعـلى الرغم من ذلـك تبينّ أنه هـدف غير واقعـي[113]، إلا أن الجهود نجحت في اكتشاف بعض ممارسي تبييض الأموال، ما جعلها تستمر.

في الولايـات المتّحدة، تسـتخدم الرقابة بوتـيرة أعـلى[114]، وتطبّق على حالات تتكاثر باسـتمرار، وتسـتعمل في تهم تتوسّـع دائرتها باطّراد؛ بل إن ذلك بات يجري أكثر من أي وقت مضى. أُعطيَت سـلطات الرقابة سنداً قانونيّاً في «قانون باتريوت» بوصفها شـأناً أساسـيّاً في مكافحة الإرهاب، وكذلك بالنسبة لمذكّرات التفتيش من النوع المعروف باسم «تسلّل وتلصّص»؛ وكلاهما بات شائعاً استخدامه خارج إطار مكافحـة الإرهـاب، كعمليات التفتيش عن المخـدّرات. في 2011، خُوّلَت «وكالة الأمـن القومي» سـلطة الرقابة على مهـرّبي المخدّرات، إضافة إلى المشـاغل التقليديّة للأمـن القومي[115]. وصدرت توجيهات إلى موظفـي «وكالة مكافحة المخدّرات» بأن يكذبوا في المحاكم؛ بهدف إخفاء أن «وكالة الأمن القومي» كانت تمرّر معلومات إليهم[116].

هنالك ما تطلق «وكالة الأمن القومي» عليه تسمية «البنية الموازية»[117]. ويقصد من ذلك أن المؤسّسـات التـي تتلقى معلومات من الوكالة، يجـب عليها أن تصطنع سُـبُلاً أخـرى يمكن الإشـارة إليها علانية بوصفهـا مصدراً للمعلومـات. الأرجح

أن الوكالـة أمدّت الـ «إف بي آي» بالمعلومات التي سـمحت للأخيرة بإلقاء القبض على قرصان الكومبيوتر روس أولبريشت، المعروف باسم «دريد بايرت روبرتس»، الذي أدار موقعاً شـبكيّاً اسـمه «طريق الحرير» من دون أن يعرّف عن هويته، يهدف إلى تمكين الناس من شراء المخدرات وغيرها من المواد الممنوعة[118].

وتُلاحَظ ظاهرة «زحف المهمة» أيضاً في المملكة المتّحدة التي تستغل فيها الرقابة المختصّة باقتلاع الإرهابيّين[119]، في العمل ضد أشخاص يهرّبون التبغ، أو يزوّرون العناويـن أو لا يهتمـون بتنظيـف مخلّفات كلابهم وغيرهـا من التجـاوزات اليوميّة البسيطة[120]. إذ تمتلك البلاد كميات كبيرة من كاميرات الرقابة، ما يجعل «منطقيّاً» استعمالها بأكثر الطرق تنوّعاً.

هنـاك أمثلـة كثيرة تأتي مـن بلدان مختلفـة. مثلاً، تجمـع إسرائيـل معلومات عن فلسطينيّين أبرياء بغرض اضطهادهم سياسيّاً[121]. وفي ظل الوسائل التقنيّة للرقابة، يسـهل الادّعاء بانزلاق الناس والمنظّمات إلى وضع إساءة الاستخدام. بديهي القول إن الحكومـات الأقـل شرعيّة تلجـأ إلى الرقابة كجـزء من تصرّفاتهـا، في ظل غياب الحماية القانونيّة لمواطنيها.

إنّها أشياء مهمّة حقّاً، حتى لو كنت ممن يثقون بالحكومة المتقلّدة للسلطة حاضراً. إذ يعتمد النظام المتّسـم بالقوة على المصداقية الكاملة لكل شـخص في السلطة[122]؛ ما يعني أن معظم الأشـياء تسـلك مسـاراً صحيحاً وأنها تخفض من الإساءة المؤثّرة للسلطة. يبقى هناك تفاحات فاسدة دوماً، فيكون السؤال فعليّاً هو عن مدى الضرر الذي يُسـمَح لها بـأن تُحدِثه بما تملكه من قـوة، إضافة إلى مدى فسـاد بقيّة الصندوق بأكمله. يفترض بالضوابط أن تعمل بكفاءة، سـواء أكنا متوافقين مع الحزب الحاكم أم لا.

تقليص حرية الإنترنت

في 2010، ألقت وزيرة خارجية أميركا آنذاك السيّدة هيلاري كلينتون خطاباً أعلنت فيه أنّ حريّة الإنترنت هدف رئيس في السياسة الخارجيّة لأميركا[123]. ولبلوغ تلك الغاية، تموّل وزارة الخارجيّة وتدعم مجموعة من البرامج العالميّة[124]، وتعمل على محاربة حجب الإنترنت، وتعزّز التشفير، وتعزّز إخفاء الهويّة. وتهدف تلك الأشياء كلها إلى «تمكين كل طفل يولد في أي مكان في العالم، من الوصول إلى الإنترنت العالميّة بوصفها منصّة مفتوحة تتيح حرية الإبداع والتعلّم والتنظيم والتعبير عن الذات، من دون حجب ولا تدخّل غير مناسب». لقد نُسِفَت تلك الأجندة عندما تبيّن بغرابة أن الولايات المتّحدة وغيرها من الحكومات الديمقراطيّة، مارست رقابة على الإنترنت من النوع نفسه الذي تنتقد ممارسته في البلدان الأكثر قمعيّة.

واغتنمت تلك البلدان القمعية الفرصة السانحة للتذرّع بالرقابة الأميركيّة في تبرير سياساتها الجائرة تجاه الإنترنت: رقابة أشد، حجبا أعتى ومزيداً من الانعزاليّة؛ وكلها توصل إلى إعطاء كلٍ من تلك البلدان سيطرة أشد صرامة على ما يقوله مواطنوها أو يفعلونه. ومثلاً، إحدى ذرائع الحكومة المصريّة لخططها بشأن فرض رقابة على الـ «سوشال ميديا»، هو القول إن «أميركا تتنصّت على المكالمات الهاتفيّة، وتتعقب كل شخص يسعى إلى النيل من أمنها القومي»[125]. ويخشى الهنود أن تستخدم حكومتهم أفعال الولايات المتّحدة لتبرير الرقابة في الهند[126]. وندّدت الصين وروسيا علانية بالنفاق الأميركي[127].

ويؤثّر ذلك في حريّة الإنترنت عالميّاً. تاريخيّاً، أُسنِدَت حوكمة الإنترنت- بغض النظر عن ضآلتها أصلاً- إلى الولايات المتّحدة؛ لأن الجميع يعتقد بأن الأميركيّين يعملون لمصلحة حرية الإنترنت، وليس بالضد منها. وأما حاضراً، بعد أن فقدت الولايات المتّحدة كثيراً من مصداقيتها، دخلت حوكمة الإنترنت في مرحلة

الاضطراب. وتسعى مؤسّسات تشريعيّة مؤثّرة في الإنترنت إلى صوغ تصوّر عن نوع القيادة الملائم لتلك الشبكة. وتحاول المنظّمات المعياريّة الدوليّة القديمة أن تؤثّر في حوكمة الإنترنت بتطوير مجموعات من القوانين القوميّة لتلك الشبكة.

يمكن اعتبار ذلك بوصفه حراكاً باتجاه السيادة الإقليميّة- القوميّة على الإنترنت، ويهدّد بتفتيتها. ليس ذلك بالأمر الجديد، لكنه لقي دفعاً هائلاً مع الكشوفات بصدد تجسّس «وكالة الأمن القومي» على الإنترنت. تجهد دول كروسيا والصين والمملكة العربيّة السعوديّة، في الدفع باتّجاه زيادة السيطرة المستقلّة على أجزاء الإنترنت التي تمر في أراضيها.

في حال تحقّق ذلك، تكون كارثة. في أساس الإنترنت أنّها منصّة عالميّة. وفي ما تستمر البلدان في الرقابة والحجب، ما زال بإمكان الشعب في البلدان القمعيّة أن يقرأ مزيداً من المعلومات وأن يتبادل الأفكار مع بقية شعوب العالم. تمثّل حريّة الإنترنت قضيّة لحقوق الإنسان، وهي جديرة بأن تلاقي دعماً من الولايات المتّحدة.

وعلانية، حضّ مؤسّس «فيسبوك» مارك زوكربرغ إدارة أوباما على ذلك، وكتب: «يجدر بحكومة الولايات المتّحدة أن تكون البطل في الدفاع عن الإنترنت، لا أن تكون تهديداً لتلك الشبكة»(128). إنّه محق تماماً.

8

العدالة التجاريّة والمساواة

عملَت مؤسّسة «آكريتف هيلث» (Accretive Health) المختصّة في تحصيل الديون، لدى عدد من المستشفيات في ولاية «مينسوتا»[1]. وتولّت مسؤوليّة الفواتير وتحصيلها في تلك المستشفيات، إضافة إلى وضع جداول العمل، وترتيبات إدخال المرضى، وخطط الرعاية الصحيّة، وتحديد مدد بقاء المرضى في المستشفى. إذا بدا أن المسألة فيها تضارب في المصالح، فالأرجح أنّها كانت كذلك. تولّت الوكالة أيضاً جمع معلومات موسّعة عن المرضى ووضعتها في خدمة غاياتها الخاصة، دون أن تفصح للمرضى عن طبيعة مسؤوليتها في الرعاية الصحيّة المقدّمة لهم، إذ استخدمت معلوماتها عن ديون المرضى في ترتيب خطط علاجهم، وضغطت على المرضى في غرف الطوارئ للحصول على الأموال. أنكرت الوكالة أنها أساءت التصرّف، لكن العام 2012 شهد تسوية قضائيّة في «مينسوتا» فرضت إبعاد الشركة عن تلك الولاية لما يتراوح بين سنتين و6 سنوات[2]. من ناحية، يدل ضبط «آكريتف هيلث» متلبّسة بأخطائها ثم توقيع عقوبة قضائيّة عليها إلى أن النظام يعمل بشكل جيّد. من ناحية ثانية، تدل تلك القضية على سهولة إساءة استخدام المعلومات عنا.

تشهد قصص مماثلة لما حدث مع «آكريتف هيلث» على وجود خطر فعليّاً على المجتمع من السماح للشركات بالرقابة العامة؛ إذ تساهم الرقابة الواسعة التي تنهض بها الشركات في الإساءات التي توجّه إلى الحريّات المدنية، والتقدّم الاجتماعي

والحرية؛ وفق ما سبق أن وصفته في الفصل السابق. وإضافة إلى مساهمتها في الرقابة الحكوميّة، تحمل رقابة الشركات مخاطرها الخاصة أيضاً.

التمييز المستند إلى الرقابة

بطريقة أساسيّة تماماً، تستخدم الشركات بيانات الرقابة في التمييز[3]، إذ تصنّف الناس ضمن فئات مختلفة، وتسـوّق السـلع والخدمات إليهم بطرق متمايزة، استناداً إلى معلومات الرقابة.

في ستينيات القرن العشرين، استخدم تعبير «بواسطة الخطوط الحمر»[4] لوصف ممارسـة تمييزيّة قديمة: تعمّد البنوك ممارسـة التمييز ضد أفراد الأقليات الإثنيّة لدى محاولتهـم شراء منازل. لم تكن البنوك لتوافق عـلى إعطاء رهونات عقاريّة في مناطق قريبة من أحياء الأقليّات- لذا كانت ترسم خطوطاً حمراً على خرائط البنوك لإظهار تلـك المناطق. وكذلك كانت البنوك لا توافق على رهونات عقاريّة لأفراد الأقليات إلا إذا كانـوا بصـدد شراء منـازل في أحيـاء تقطنهـا غالبيـة من الأقلية التـي ينتمون إليهـا. بالطبـع، لم يكـن ذلك شرعيّاً، لكن البنوك مارسـته لفترة طويلـة من دون أن تعاقب عليه. وبصورة أكثر تعميماً، يمكن القول: ممارسة رسم الخطوط الحمر تعني الإمسـاك عن تقديم خدمات [أو تقديمها بأسـعار مبالغ فيها] مع اسـتخدام مكان السكن كاسم آخر للعرق- وهو أمر تزيد سهولته كثيراً باستخدام الإنترنت[5].

في العام 2000، أنشأ بنك «ويلز فارغو» موقعاً إلكترونيّاً للترويج لعروضاته في الرهونات العقاريّة[6]. وقدّم الموقع «آلة حاسـبة مجتمعيّة» لمساعدة الشُراة المحتملين في التعـرف إلى الأحيـاء التي يحتمل أن يقطنوها. وتحتسـب تلك الآلـة أرقام البلديّة الحـاضرة للـشراة المحتملـين، وترشـدهم إلى أحيـاء تنسـجم مع العـرق المهيمن في الأحياء التي تدل عليها أرقام البلدية الحالية للساعين إلى الشراء. بمعنى آخر، عمل الموقع على إرشـاد المشـترين الآتين من أحياء تسـكنها غالبية من البيض إلى منازل في أحياء مماثلة، وكذلك الحال بالنسبة لأصحاب البشرة السمراء.

تسمّى تلك الممارسة بواسطة «خطوط الويب»[7]، وتملك قدرة كامنة على ممارسة التمييز بطرق أشد وأكثر توسّعاً من سياسة «بواسطة الخطوط الحمر» التقليديّة. ولأن الشركات تجمع معلومات وافرة جداً عنّا، وتستطيع وضع ملفّات عن صفاتنا الشخصيّة؛ لذا تتمكن من التأثير فينا بطرق متنوّعة. وفي 2014، خلص تقرير صادر عن البيت الأبيض بشأن «البيانات الضخمة» إلى القول إنّ «الأدوات التحليليّة في البيانات الضخمة تملك القدرة على الإزراء بكل أنواع الحماية للحقوق المدنيّة، المتعلّقة بطُرُق استخدام المعلومات الشخصيّة في الإسكان والإقراض والتوظيف والصحة والتعليم والسوق»[8]. أميل للاعتقاد بأن التقرير تفهّم خطورة «البيانات الضخمة».

يشكّل التمييز في الأسعار شيئاً فائق الأهمية حاضراً. إذ يتجاوز التمييز التقليدي في العرق ونوع الجنس مثلما يحصل في «بواسطة خطوط الويب»؛ لأنه يتضمن أن تعطي الشركات أسعاراً متفاوتة لفئات مختلفة من الناس كي تحصل على أقصى قدر من الأرباح. باتت تلك الممارسة شبه مألوفة في حجوزات الطيران. إذ تتغيّر الأسعار باستمرار اعتماداً على عناصر من نوع كم ندفع مقدّماً، في أي الأيام نسافر ودرجة امتلاء الطائرة بالركاب.

تهدف شركات الطيران من تلك الممارسة إلى بيع تذاكر السفر بأسعار تفضيليّة إلى من يقضون إجازاتهم في الخارج ما يجعل هؤلاء *يقبلون* شراءها. في المقابل، تستخرج من المسافرين لإنجاز الأعمال أرباحاً أعلى طالما أنهم *يقبلون* دفعها. لا يوجد ما هو شيطاني في تلك الممارسة باعتبار أنها تتعلّق بمضاعفة العائدات والأرباح. وعلى الرغم من ذلك، لا يحوز التمييز في الأسعار شعبيّة كبيرة عند الناس. ومثلاً، يوصف رفع سعر مجارف الثلج بعد عاصفة ثلجيّة بأنّه تسعير ابتزازي. ولذا، يجري تمويهه ضمن عروض خاصة، أو منح كوبونات أو بطاقات استرجاع المال.

هناك أنواع غير قانونيّة من التمييز بالأسعار. ومثلاً، لا يستطيع المطعم أن يمارس تمييزاً بالأسعار استناداً إلى العرق أو النوع الجنسي للزبون. في المقابل، يستطيع وضع أسعار تتغيّر وفق أوقات تناول الطعام، وهو سبب وضع أسعار مختلفة لوجبتي الغداء والعشاء على الرغم من احتوائهما الأطباق عينها. ويعتبر أمراً قانونيّاً أن تعطى أسعار وجبات تفضيليّة للمسنين، وكذلك الحال بالنسبة لوجبات الأطفال. ويندرج ضمن الممارسة القانونيّة فرض شركة «أوبر» أسعاراً أعلى لتوصيلاتها في أوقات الذروة في حركة المواصلات[9].

في أعمال كثيرة، تُقدّم لك عروض، وتُمنح لك أسعار وتحصل على خدمات، استناداً إلى المعلومات عنك. يشمل ذلك قروض البنوك، التأمين على السيارة، بطاقات الائتمان وما إلى ذلك. تسهل رقابة الإنترنت الضبط الدقيق لتلك الممارسة. وصار سائداً على الشبكة أن يعرض الباعة الإلكترونيّون عليك أسعاراً وخيارات متنوّعة، استناداً إلى تاريخك وما يعرفونه عنك[10]. واعتماداً على من تكون[11]، ربما ترى صورة لسيارة حمراء بسقف متحرك أو سيّارة عائليّة من نوع «ميني- فان» في ما يصلك من إعلانات السيّارات، وكذلك تعطى خيارات مختلفة في سداد الثمن والتخفيضات، عند زيارتك لموقع موزع السيّارات. ووفق مقال ظهر في صحيفة **وول ستريت جورنال (Wall Street Journal)** في 2010، فإن الأسعار التي يعرضها عليك موقع «ستابلز» للشراء الإلكتروني بالمفرّق، تعتمد على مكان سكنك، ومدى قرب محل منافس من منزلك. ويورد المقال عينه أن شركات كبرى للمبيعات كـ«روزيتا ستون» و«هوم ديبو»، تمارس أيضاً سياسة تغيير الأسعار وفقاً للمعلومات الفرديّة عن المستهلك[12].

وبصورة أوسع، لكل منا سجله كزبون[13]. ويربط سماسرة المعلومات ذلك الملف بكل واحد منا. ويشبه السجّل جداول بطاقات الائتمان، لكنه لا يتألف من عنصر مفرد [كالمال في تلك البطاقات]، بل يركّز على ما تشتريه استناداً إلى أشياء كالبيانات عما اشتريته من مخازن البيع بالتجزئة، المعلومات عن وضعك المالي، البيانات الآتية

من استطلاعات الرأي، وبيانات تسجيل بطاقات ضمان السلع، التفاعلات المختلفة بواسطة الـ «سوشال ميديا»، وبيانات بطاقات ولاء المستهلك، السجلات العامة، تفاعلاتك مع مواقع الإنترنت، قوائم الأعمال الخيريّة، اشتراكاتك على الـ «ويب» وخارجه أيضاً، والبيانات عن صحّتك ولياقتك. وتستعمل تلك المعلومات كلها لتحديد نوع الإعلانات والعروض التي ستشاهدها أثناء تجوالك في الإنترنت.

في العام 2011، كوّن الجيش الأميركي مجموعة من إعلانات التطوّع، تُظهِر جنوداً من إثنيات وهويات جنسيّة مختلفة[14]. وتشارك مع إحدى شركات الكابل في توزيع تلك الإعلانات بما يتوافق مع المعلومات الديموغرافيّة عمن يسكن كل منزل على حِدَة.

هنالك طُرُق أخرى في التمييز. في 2012، وضع فندق «أوربتز» أسعاراً متباينة لغرفه، تميّز بين النزلاء الذين يستخدمون نظام «ويندوز» وأولئك الذين يستعملون نظام الـ «ماك»[15]. وتتقصّد مجموعة من المواقع الشبكيّة للسفر والسياحة إظهار صفقات مختلفة لزوّارها؛ استناداً إلى تاريخ التصفّح لكل زبون[16]. وتستند بعض المواقع إلى معرفتها بالمستوى الاقتصادي لزوّارها، فتظهر لهم صفحات تتوافق مع مستوى دخلهم. يبدو كثير من تلك الأشياء مرهفاً تماماً. إذ لا تعني تلك الممارسات أنك لن تشاهد أسعار رحلات سياحيّة أو غرفاً فندقيّة معيّنة، بل أن يضع الموقع ترتيباً لتسلسل ظهور صفحاته بما يتّفق مع معلوماته عن زائريه، مع افتراض أن الزبون يختار الأكثر سهولة بالنسبة له. وفي الفصل 3، رأينا أنّ بياناتنا يمكن استعمالها لمعرفة العمر والنوع والخيار الجنسي، وحال العلاقات الخاصة وأشياء كثيرة أخرى. يعطي ذلك الوضع للشركات اليد العليا على حساب جمهور المستهلكين، ومع استمرار الشركات في مراكمة المعلومات عن الأفراد والطبقات؛ تتزايد سيطرتها وتتقوّى باطّراد. ومثلاً، يعلم المسوّقون أن المرأة تحس بأن جاذبيّتها تكون أقل يوم الاثنين باعتباره بداية أسبوع العمل، فترى الشركات فيه اليوم المناسب لإمطارهن بإعلانات عن مواد التجميل[17]. وكذلك تعلم الشركات أن ردود الفعل على

إعلاناتها تتفاوت وفق العمر ونوع الجنس[18]. ومستقبلاً، ربما أصبحت معلومات الـشركات عن الأفـراد أكثر دقّة، ما يزيد مـن دقّتها في توجيـه إعلاناتها. إذا علمت الـشركات أنّـك في الثامنة صباحـاً تكون مشوشـاً لأنّك لم تتنـاول قهوتك، تتجنّب إرسال إعلاناتها إليك في تلك الساعة. وتنطلق إعلاناتها إليك في التاسعة والنصف، بعد أن تفعل القهوة فعلها، ثم تتجنّبك بعد الساعة 11 نهاراً؛ لأن شيئاً من التشوش يعود إليك مع انخفاض مستوى السكر في دمك قبيل موعد الغذاء.

وكذلك يجري الحكم على الناس وفقاً لشبكة علاقاتهم على الـ «سوشال ميديا». تعمـل شركـة «لينـدو» الفليبينيّـة عـلى تقييم صلاحيـة الأفـراد للقـروض، بتدقيق الوضعيـة الماليّـة لمن يتفاعلون معهم باسـتمرار عـلى «فيسـبوك»[19]. وفي مثل آخر عـلى التمييز «بواسـطة خطوط الويب»، تخفض شركة «آميركان إكسـبرس» سـقف بطاقات الائتمان وفقاً لنوع المتاجر التي يتسوّق منها طالب البطاقة[20].

قدّم البروفسـور أوسكار غندي، وهو أستاذ قانون في «جامعة بنسلفانيا»، وصفاً مبكّـراً عـن ذلك الوضـع برمّته، إذ سـمّاه في 1993 «الفـرز بالرؤية الشـاملة»[21]، مشـيراً إلى «عمليات تجميـع المعلومات وتحليلها ومشـاركتها، وهي تشـمل الأفراد والمجموعات. ويجري توليد تلك المعلومات في سياق الحياة اليوميّة للناس بوصفهم مواطنين وموظّفين ومستهلكين. وتستخدم المعلومات في السيطرة على مدى وصولهم إلى البضائع والخدمات التي تحدّد الحياة في الاقتصاد الرأسـمالي المعاصر». من المؤكّد أن من يملكون ذلك النوع من السـلطة، يمتلكون سـلطة ضخمة فعليّاً. إنها سـلطة استعمال مؤشّرات تمييزيّة لتوزيع الفرص والوصول والاستحقاق والأسـعار[22] (غالبـاً مـا تكون على هيئة عروض خاصـة وتخفيضات) والاهتمام (إيجابيّاً وسـلبيّاً) والتعرّض للمعرفة.

مـن المحتمل أن تغدو تلك الممارسـة تدخليّـة جداً. إذ شرعـت المطاعم الفاخرة في التفتيش عن معلومات عن أسـماء زبائنها بواسـطة «غوغل»؛ بهدف تحسين تجربة

تناول الطعام فيها[23]. إنّها لا تستطيع أن تعطي الوجبات نفسها بأسعار متفاوتة، لكنها تقدر أن تقدّم قائمتها للمشروبات الروحيّة أنواعاً باذخة أو رخيصة. وتجرب شركات تأمين المركبات يدها في ربط التأمين بأداء الزبون على الطرقات. إذا سمحت لشركة التأمين أن تعرف أوقات قيادتك لمركبتك، والمسافات التي تقطعها، وسرعتك في القيادة؛ فلربما حصلت على تأمين بأقساط أرخص[24].

تزيد إمكانات التدخل بصورة كبيرة في إطار علاقة الموظّف برب العمل. ثمة شركة واحدة على الأقل فاوضت على إمكان توزيع سوارات «فِت بت» الرقميّة التي تقيس مؤشّرات الصحة الجسديّة على موظّفيها، مع إعطاء شركات التأمين الصحي معرفة غير مسبوقة تاريخيّاً عن العادات الصحيّة للزبائن بسوارات «فِت بت»[25]. وعلى نحو مماثل، تفرض ثانويات كثيرة على طلبتها ارتداء مجسّات ذكيّة لقياس دقّات قلوبهم أثناء ممارسة الرياضة، لكنها لا تنطق ببنت شفة عن طريقة استخدام تلك البيانات بعد تجميعها[26]. في 2011، حلّلت شركة «هيوليت باكارد» الشهيرة في صناعة الكومبيوتر بيانات موظّفيها كي تعرف من موشك على تركها، ثم لفتت أنظار المدراء إليهم[27].

تشكّل الرقابة في مواقع العمل حقلاً جديداً محمّلاً بإمكانات ضخمة في الأذيّة[28]. بالنسبة للعديدين منّا، يعدُّ رب عملنا هو السلطة الأكثر خطورة في مراقبتنا[29]. وتشمل قائمة الموظّفين المعرضين للرقابة المنتظمة، موظّفي مراكز المكالمات الهاتفيّة، سائقي الشاحنات، عمال الصناعة، طواقم المبيعات، عمال البيع بالتجزئة، وغيرهم. وتتزايد أعداد من يتعرّضون لرقابة إلكترونيّة مستمرة، من قِبَل الشركات التي يعملون فيها. تأتي معظم تلك الأشياء من حقل جديد يسمّى «تحليلات موقع العمل»، وهي أساساً إدارة الموارد البشريّة استناداً إلى معلومات الرقابة[30]. إذا استعملت الاتّصالات الإلكترونيّة للشركة كالحاسوب والخلوي، فأنت تعطي مديرك الحق في معرفة كل ما تفعله على تلك الأجهزة[31]. يمتلك بعض تلك الممارسات شرعيّة، فمن حق رب العمل أن يضمن أنّك لا تمارس لعبة

«فارم فيل» (Farmville) الشـهيرة طيلة اليوم. لكنك ربما استخدمت تلك الأجهزة في أوقاتك الخاصة، لإنجاز اتّصالات بعضها خاص والآخر متّصل بالعمل.

كلما تعرّضنا للرقابة والتصنيف المستند إليها، تزايد إمكان أن تسير الأمور في مسار الخطأ. هناك مثل صار مألوفاً لديك: فكّر بكل تلك الإعلانات الفائضة التي تتدفق إليك بواسطة الإنترنت مستندة إلى تحليلات حسابيّة ربما تسيء التعرّف إلى اهتماماتك. يتقبّل بعض الناس ذلك، فيما يمثّل لآخرين أذيّة نفسية منخفضة المستوى، تتأتى من استعمال البيانات لتصنيفهم ووضعهم في فئات، سواء عن حق أم باطل[32]. ويتزايد إمكان حدوث الأذى كلما كان الحكم على الشخص له أهمية أكبر، كأن يصنّف الأفراد في فئات بالنسبة للقروض الائتمانيّة استناداً إلى أرقام وجداول خوارزميّة، وكذلك تعتمد طريقة تعامل قوى الأمن معنا في المطارات على المعلومات التي جمعتها الشركات عنّا، ولو بصورة جزئيّة.

يترتب على ذلك الوضع آثارٌ مفزعة اجتماعيّاً. إذ يعزف الناس مثلاً عن التفتيش عن معلومات حول أمراضهم؛ خوفاً من وصول بيانات عمليات التفتيش على الإنترنت إلى شركات الضمان الصحي، ما يؤدّي إلى إخراجهم من شبكة ذلك الضمان[33].

ويصح القول إنّ جزءاً كبيراً من التصنيف الذي تنهض به الشركات يبدأ بنوايا طيّبة. فلربما حُرِم أناسٌ من قروض بنكيّة بسبب الإنهاك المالي لأصدقائهم على «فيسبوك»، لكن النظام الذي صنعته شركة «ليندو» الفليبينيّة [انظر أعلاه] يسمح بإقراض من ليس لهم تصنيف ائتماني: إذا كان لأصدقائهم وضع ائتماني جيد جيداً، يسجل ذلك كعلامة لصالحهم. وفي طيّات استخدام المعلومات الشخصيّة في تحديد نسب التأمين أو سقف الائتمان المالي، أن بعض الأشخاص ربما حصلوا على صفقات أسوأ من تلك التي كان ممكناً أن ينالوها لولا المعلومات الشخصيّة عنهم، فيما يكون الوضع معكوساً بالنسبة لكثيرين أيضاً.

وبصورة عامة، تستعمل الشركات الكبرى بيانات الرقابة لزيادة أرباحها على حساب الزبائن[34]. ولا يستسيغ الزبائن ذلك، ولكن طالما أنّ (1) الباعة يتنافسون بين بعضهم بعضاً للحصول على أموالنا، و(2) شركات المعلوماتيّة تصنع برامج تسهّل ممارسة الأسعار التمييزيّة، و(3) التمييز يجري خفية عن الزبائن؛ يكون من الصعب على الشركات مقاومة إغراء تلك الممارسة.

التلاعب استناداً إلى الرقابة

من يمتلك معلومات عنّا يمتلك قدراً من التحكّم بنا، ومن يعرف كل شيء عنا يمتلك قدرة كبيرة على التحكّم بنا. بالاختصار، الرقابة تسهّل التحكّم.

ليس ضروريّاً أن يشمل التلاعب الإعلان المباشر. إذ يمكن أن يكون ترتيباً للمنتجات يجعلك ترى صوراً تظهر في خلفيتها سيّارة من ماركة معيّنة. ولربما اقتصر أمره على الوتيرة التي ترى فيها تلك السيّارة. وأساساً، يمثّل ذلك نموذج العمل لدى محرّكات البحث على الإنترنت. وفي أزمانها الأولى، تداولت المحرّكات كلاماً عن إمكان أن يدفع المعلِنون أكثر مقابل ظهورهم أولاً في نتائج عمليات التفتيش بتلك المحرّكات[35]. وبعد احتجاج من الجمهور أودى إلى صدور توجيهات من «اللجنة الفيدراليّة للتجارة»، لجأت محرّكات البحث إلى التمييز بصريّاً بين النتائج التي تأتي «طبيعيّاً» من الجداول الخوارزميّة، وتلك التي توضع في الصدارة لأنها مدفوعة[36]. وحاضراً، تظهر النتائج المدفوعة في مربّعات صُفْر على محرّك «غوغل»، فيما يضعها محرّك «بينج» في مربّعات ملوّنة بالأزرق الخفيف. وسرت الأمور كذلك لفترة معيّنة، ثم انتقلت الأمور إلى وضعها السابق في الآونة الأخيرة. إذ بات «غوغل» يتلقى أموالاً لقاء وضع روابط إلكترونيّة لمواقع معيّنة في مركز متقدّم من نتائج البحث، ولم يعد يكتفي بوضعها في مساحة إعلانية منفصلة[37]. لا نعلم المدى الذي ستذهب إليه الأمور، لكن «اللجنة الفيدراليّة للتجارة» شرعت في الاهتمام به أيضاً[38].

عندمـا تقلّب المواد التي تصل إلى صفحتك على «فيسـبوك»، فأنت لا تطالع كل تدوينـة ومَنْ كتبها؛ بالأحـرى أنت تطالع المواد وفق ترتيب تعـدّه في دواخل الموقع جـداول خوارزميّـة مؤتمتـة لا يُصار إلى كشـفها للعمـوم. ولكن، تذكّـر أن هنالك مـن هم مسـتعدون لأن يدفعوا لقـاء أن تكون تدويناتهم [«بوسـت»] أول ما يقرؤه الأصدقاء أو المعجبون على صفحاتهم. يشكّل ذلك النوع من الدفع مقابل التموضع شـطراً أساسـيّاً من مداخيل «فيسـبوك»[39]. وعلى غرار ذلك، فـإن معظم الروابط الإلكترونيّـة التي توصـل إلى المقالات الإضافيّة في صفحة الأخبـار، إنّما هي روابط دفع أصحابها لقاء ذلك التموضع.

هناك كثير من التلاعب كامن في ذلك السياق. إليك أحد النماذج. في الانتخابات الرئاسيّة للعام 2012، نال مستخدمو «فيسبوك» إمكان وضع أيقونة «أنا اقترعت»، تشـبه كثيراً تلك اللصقة التـي نحصل عليها بعد وضع الورقـة في صناديق الاقتراع فعليّـاً. هنالك تأثير الالتحـاق بالآخرين الذي أثبتته وثائق كثـيرة، بمعنى أنّك تميل أكثـر إلى التصويت لدى معرفتك بأن أصدقـاءك صوّتوا قبلك. أدى ذلك التلاعب إلى زيادة الإقبال على التصويت بمعدل 0.4 ٪ على مسـتوى الولايات المتّحدة[40]. لا شيء مؤذٍ في ذلك، عند هذه النقطة. لكن، تخيّل لو تلاعب «فيسبوك» بأيقونة «أنا اقترعـت» إمـا وفق الانتـماء الحزبي، أو بعض بدائلـه المقبولة كأرقـام المناطق البلديّة للمنـازل، أو نـوع المُدوّنات المفضلـة أو الروابط الإلكترونيّة التـي أبدى إعجابه بها وغيرها. لم يفعل «فيسبوك» ذلك، لكن لو أنّه فعل لتمكن من تغيير معدل التصويت لمصلحـة تيـار معيّن. وكذلك لكان من الصعب اكتشـاف ذلك، بل إنه ربما لا يكون غير قانوني[41]. يسـتطيع «فيسـبوك» أن يقلب اتجاه التصويـت في انتخابات متقاربة النتائـج، بالتلاعـب بالأولويّة التي يرى فيهـا الجمهور تدوينات الـ «بوسـت» على صفحاتهم[42]. وربما يفعل «غوغل» أمراً مُشـابهاً بواسـطة التلاعب بنتائج عمليات التفتيش عليه[43].

إذا عقـدت إحـدى المنصّـات السـيّئة النوايا في الـ «سوشـال ميديـا» عزمها على التلاعـب بالـرأي العـام، فبإمكانهـا أن تمضي أبعد مما سـبق وصفه[44]. إذ تسـتطيع تضخيـم أصـوات النـاس الذيـن تتوافق معهـم، وتهمّش مـن لا تتوافـق معهم، ما يعطيها القدرة على تحريف مسـار الجمهور. فعلت الصين ذلك بـ «حزب الخمسـين بالمئة» (50 Cent Party)[45]. وفي الصين، تستخدم التسمية في الإشارة إلى أشخاص اسـتأجرتهم الحكومة لنشر تدوينات [«بوسـت»] مؤيّدة للحزب الشيوعي الصيني عـلى الشـبكات الاجتماعيّـة، وتحـدي التعليقـات المعارضـة لمواقف ذلـك الحزب. وانخرطت شركة «سامسونغ» في أمر مُشابِه تماماً[46].

وفقاً للملف الشـخصي كمسـتخدم للإنترنت، تتلاعـب شـركات عـدّة في مـا تـراه على الشـبكة[47]: عمليات البحث التي أجريتها عـلى «غوغل»، والأخبار التي طالعتها على «ياهوو»، وحتى وتيرة مطالعتك لصحف كبرى مثل نيويورك تايمس. إنّـه لأمر جلـل. إذ تحصل الصفحـة الأولى من نتائج البحـث في «غوغل» على ثلث إجمالي المشاهدات[48]؛ فإن لم تكن على الصفحة الأولى، فالأرجح أنّك غير موجود. وبالنتيجـة، صـارت الإنترنـت التي تراها أكثر ميـلاً لأن تكون مفصّلـة على مقاس ملف ملامحك الشخصيّة مع ما يتضمّنه من مؤشّرات على مصالحك[49].

ويقـود ذلك إلى ظاهرة سـمّاها الناشـط السـياسي الأميركي إيلي باريـزر «فقاعة الفلـتر»[50]؛ بمعنـى أن تصلـك «إنترنت» تكون مفصلة على مقـاس خياراتك، فلا تطالع أبداً رأياً لا يتّفق مع توجّهاتك. ربما ظننت أن ذلك الأمر ليس سيئاً، لكنه مؤذٍ تماماً على المسـتوى الواسـع[51]. إذ لا نرغب في العيش في مجتمـع لا يقرأ فيه الجميع طيلة الوقت إلا الآراء التي تدعم آراءهم[52]، وليس الحال فعليّاً أننا لا نتعرّض أبداً لتلك المواجهات التي تجدّدنا وتوافقنا وتتحدّانا وتعلّمنا.

في 2012، أجـرى «فيسـبوك» تجربـة أبقاهـا تحـت السـيطرة[53]. إذ تلاعـب بالتدوينـات التـي تصـل وتتجدّد عـلى صفحات 680 ألـف مسـتخدم، مُظهِراً لهم

تدوينات إما أكثر سعادة أو أشد تعاسة. ولأن «فيسبوك» يقيم مستخدميه باستمرار- وهي الطريقة التي يستخدمها في جعل جمهوره مورداً إعلانياً- كان من السهل عليه تقييم الأشخاص المشمولين بالتجربة، وتجميع النتائج. وتبيّن لـ «فيسبوك» أن الأشخاص الذين وصلتهم تدوينات سارة بوتيرة أعلى، كتبوا تدوينات أكثر سعادة، والعكس بالعكس. لا أرغب في المجادلة طويلاً بشأن تلك النتيجة. ولم تستمر تجربة «فيسبوك» إلا أسبوعاً وخلّفت آثاراً ضئيلة. في المقابل، بمجرد أن تفهم مواقع كـ «فيسبوك» كيف تستطيع فعل ذلك بكفاءة، فسرعان ما ستحوّلها مصدراً للمال. لا تشعر النساء أنّهن أقل جاذبيّة يوم الإثنين فحسب، بل يشعرن بذلك أيضاً عندما يكُنّ مكتئبات[54]. ونشهد حاضراً بدايات نُظُم تحلّل الصوت وحركات الجسد كي تحدّد الحال المزاجيّة للشخص. وكذلك ترغب الشركات في معرفة متى يكون زبائنها أكثر إحساساً بالإحباط، ومتى يكون مجزياً زيادة عرض المبيعات لهم[55]. ويشكّل التلاعب بالحال المزاجيّة بالتوافق مع منتجات السوق أمراً يرغب فيه عالم الإعلانات مهما بدا ذلك مرعباً بالنسبة لنا.

يغدو التلاعب أسهل بأثر من الطابع المركز لكثير من النُظُم التي نستخدمها. وتقف شركات كـ «غوغل» و«فيسبوك» في القلب من نُظُم اتّصالاتنا، ما يعطيها قوّة كبرى في التلاعب والسيطرة[56].

هنالك أضرار فريدة من نوعها من الممكن أن تتأتى من استخدام بيانات الرقابة في السياسة. إذ تشبه إدارة الحملات الانتخابيّة تلك المتّبعة في التسويق؛ كما شرع السياسيّون في الاستفادة من القدرة الجديدة في الإعلان المشخصن كأداة لتتبع أنماط التصويت المتمايزة، و«تسويق» مرشّح ما أو موقف سياسي معيّن. كذلك يستطيع المرشّحون ومجموعات المصالح الخاصة صنع إعلانات وحملات استجلاب الأموال مفصلة على قياس مجموعات معيّنة[57]: من لديهم دخل يفوق 100 ألف دولار سنويّاً، محبّذو اقتناء السلاح، الأفراد الذين قرأوا مقالات تعبّر عن وجهة محدّدة في قضيّة ما، النشطاء المتقاعدون... بل كل ما يمكن أن تفكّر فيه. كذلك يستطيعون

توجيه إعلانات محمّلة بالغضب إلى مجموعة معيّنة، وإرسال إعلانات رزينة ومعمّقة سياسيّاً إلى مجموعات أخرى. ويتمكنون من المتابعة الدقيقة لحملات حثّ الناخبين على الاقتراع في يوم التصويت[58]؛ وكذلك إعادة تقسيم المناطق الانتخابيّة بين اقتراع وآخر بما يتلاءم مع مصلحة حزب معين[59]. تحمل تلك الأنماط من استعمال البيانات مخاطر أساسيّة على الديمقراطيّة والاقتراع[60].

وباطّراد، سوف تتحسّن القدرة على التلاعب النفسي المستند إلى المعلومات الشخصيّة والتحكّم بالنُظُم التي تعتمد المعلومات عليها. وهناك ما هو أسوأ، يتمثّل في أن التلاعب النفسي سيرتقي إلى حدّ أننا لن نشعر به. ربما يصعب علينا قبول تلك الحقيقة؛ لأننا كلنا نؤمن بأننا أذكياء بدرجة تمنع من جعلنا ألعوبة بيد آخرين. حسناً: لسنا كذلك.

انتهاكات الخصوصيّة

في العام 1995، اخترق الـ «هاكر» كيفن ميتنيك شبكة تابعة لإحدى شركات الإنترنت، اسمها «نت كوم» (Netcom)، واختطف أرقام ما يزيد على 20 ألف بطاقة ائتمانيّة[61]. في 2004، اخترقت مجموعة من الـ «هاكرز» شبكة إحدى شركات سماسرة المعلومات، اسمها «شويس بوينت» (Choice Point)، وسرقت بيانات ما يزيد على مئة ألف شخص، واستخدمتها في عمليات احتيال[62]. في أواخر 2014، اخترق الـ «هاكرز» الشبكات الداخليّة لمؤسّسة «هوم ديبو»، واستولوا على قرابة 60 مليون أرقام بطاقات ائتمانيّة[63]، وبعدها بشهر؛ أُعلِن عن عملية سطو على معلومات ترجع إلى قرابة 83 مليون أسرة كانت لدى بنك «جي بي مورغان تشيس»[64]. خلال عقدين من عمر الإنترنت، من الجلي أنه لم يتغيّر شيء سوى اتّساع مدى العمليات.

ثمة سؤال منطقي: إلى أي مدى تحمي شركات الإنترنت، وسماسرة المعلومات والمؤسسات الحكوميّة؛ معلومات الجمهور؟ ومن وجهة معيّنة، يبدو السؤال ضئيل

الدلالـة. ففـي الولايات المتّحدة، يسـتطيع أي شـخص قـادر على دفع المـال مقابل الحصـول على معلومـات أن يفعل ذلـك فعليّاً. في بعض الأحيان، اشـترى مجرمون بيانات بطريقة قانونيّة، ثم استخدموها في عمليات احتيال[65].

إنّ ظاهـرة الجريمـة السـبرانيّة أقـدم مـن الإنترنـت نفسـها، وتمثّـل أيضـاً تجارة مربحـة[66]. وإذ يصعـب الحصـول عـلى أرقـام دقيقـة، تسـهل معرفـة أنهـا تكلّف الولايـات المتّحدة عـشرات بلايين الـدولارات. ومع أرقام كتلـك، تكون الجريمة الإلكترونيّة الشبكيّة ظاهرة منظّمة ودوليّة.

يتضمّن شطر كبير من تلك الظاهرة سرقة الهويّة، ما جعل الاحتيال بهويّة منتحلة أحـد الخيالات الكبرى في عصر الإنترنت. إذ يخترق المجـرم قاعدة بيانات في مكان ما، ويسـطو على معلومات عن حسـابك البنكي وربما كلمات المرور أيضاً، وينتحل شـخصيتك للحصـول عـلى قـرض باسـمك. وربـما سرق رقـم بطاقتـك الائتمانيّة واستخدمها في التبضّع. ومن الممكن أن «يفبرك» استرداد ضرائبي باسمك ويحصل على تلك الأموال، ما يعرّضك للمساءلة القانونيّة لاحقاً[67].

ليست مسـألة شـخصيّة. إذ لا يركض المجرمون خلف معلوماتك الحميمة؛ بل جلّ ما يسعون إليه هو بيانات عن حساباتك المالية للوصول إليها. وكذلك يرومون بيانات شخصيّة تكفي للحصول على رصيدك.

قبـل حفنة من السـنين، كان الخطـر الداهم يتمثّل في إمـكان أن يخترق المجرمون حاسوبك ويسطوا على معلوماتك وبياناتك. لكن مستوى سرقة البيانات استمر في الارتفـاع مـع الزمن. وفي أيامنا، بات المجرمون أكثر ميـلاً لاختراق قواعد البيانات في الشركات الكبرى، ويسرقون معلوماتك الشخصية ضمن بيانات لملايين الناس. إنّه أمـر أكثر نجاعة. وكذلك تخترق قواعد البيانات الحكوميّة باسـتمرار[68]. ومرّة تلـو الأخرى، تعلّمنا أن بياناتنا لا تتمتـع بحماية جيّدة. تحدث سرقة البيانات بوتيرة منتظمـة بأكثـر ممـا يظهر في وسـائل الإعـلام. إذ يخبرني كثـير من المحامين لشـؤون

الخصوصيّة أن انتهاكات البيانات وهشاشاتها أكبر بكثير مما يعلن عنه- بل إن بعض الشركات لا تعي أن شبكاتها اختُرِقَت وبياناتها سُرِقَت[69]. من المذهل معرفة مدى الرداءة في أمن الشركات. ولأن المؤسّسات تحصل على بياناتك بطريقة شرعيّة، فإنّها لا تتعرض للمساءلة إذا أضاعتها.

أحياناً، لا يسعى الـ «هاكرز» خلف الأموال. ففي العام 2010، اعتُقِل مواطن من كاليفورنيا اسمه لويس ميهانغوس، بسبب «الابتزاز الجنسي»[70]. وكان يخترق حواسيب ضحاياه من الإناث، ويبحث عن صورهن الجنسيّة، ثم يتسلل إلى كاميرا الكومبيوتر ليلتقط صوراً حميمة إضافيّة لهن. وبعدها، يتّصل بهن مهدّداً بنشر تلك الصور إن لم يزودنه بمزيد من الصور والأشرطة الجنسيّة لهن. يُطلق على أمثال ميهانغوس اسم «راتر» (ratter)، اشتقاقاً من «رات» (RAT) وهي الحروف الأولى لعبارة (Remote Access Trojan) التي تعني «التسلّل عن بعد بواسطة [فيروس إلكتروني من نوع] تروجان» [= «فيروس حصان طروادة»]. ويستخدم أولئك الأشخاص فيروسات «تروجان» للتحكّم بحاسوبك، بل إن بعض الـ«راتر» الأكثر خفاءً يسيطر بتؤدة على كاميرا حاسوبك فيشغّلها عن بُعد من دون إشعال ضوء الاستعمال[71]. هناك مجموعات من الـ «راتر» لا تبتزّ ضحاياها، لكنها تتاجر بصور الناس وأشرطتها وملفاتها.

لا يقتصر أمر التسلّل عن بُعد على الـ «هاكرز». ففي الفصل 7، تحدّثت عن تلك المدرسة التي تجسّست على تلامذتها بواسطة حواسيبهم. في العام 2012، نجحت «اللجنة الفيدراليّة للتجارة» بمقاضاة 7 شركات تبيع الحواسيب بالتقسيط، لكنها كانت تتجسّس على زبائنها مستخدمَةً كاميرات الـ «ويب» في حواسيبهم[72].

أثناء تأليف هذا الكتاب، تناهت إلى مسامعي قصة مماثلة رواها شخصان مختلفان. وحكى كل منهما أن صديقاً- بالأحرى ابنته- سجلت في كليّة جامعيّة. وبعد سنوات قليلة، تلقت الابنة رسالة من كليّة لم تتقدّم إليها أبداً. ونقلت الرسالة

أن الكليّة جمعت معلومات عن الابنة خزّنتها لسنوات عدّة، وأن بعض الـ «هاكرز» دخلوا إلى قاعدة بيانات الكليّة أخيراً، وسرقوا تلك المعلومات كلها. وكذلك حملت الرسالة الابنة أن تضع تنبيهاً بحصول احتيال على حسابها مع مكاتب إقراض كبرى.

في الحالتين كلتيهما، حصلت الكليّة على معلومات عن الابنة من سمسار، عندما كانت تلك الصبيّة في نهاية المرحلة الثانويّة، سعياً لاجتذابها إلى صفوف الكليّة. وفي الحالتين، لم تكن الصبية قد حاولت أبداً الانتساب إلى الكليّة التي بعثت إليها بتلك الرسالة. ولم يحل ذلك دون تخزين الكليّتين البيانات لسنوات طويلة، وكذلك لم تقدر أيٌّ منهما على حماية تلك البيانات.

9

التنافسية التجارية

في 1993، كانت الإنترنت مغايرة تماماً لحالها حاضراً. لم تكن التجارة الإلكترونيّة قد ظهرت، وكانت «الشبكة العنكبوتيّة العالميّة»(*) (World Wide Web) تجتاز طفولتها المبكرة. كانت شبكة الإنترنت أداة اتّصال متقدّمة لا يستخدمها سوى الأكاديميّين ومحترفي التقنية الإلكترونيّة، كما كنّا نستعمل البريد الإلكتروني، ومجموعات الأخبار، إضافة إلى بروتوكول لتبادل المُحادثات يشار إليه تقنيّاً باسم «آي آر سي» (IRC). كانت الحواسيب بدائيّة، وكذلك حال أمن الكومبيوتر. وطيلة 20 عاماً، نجحت «وكالة الأمن القومي» في الإبقاء على برامج التشفير بمنأىً عن التداول الواسع؛ بتصنيفها ذخائر وبالتالي تقييد تصديرها. ولم يتسن للشركات الأميركيّة التي تنتج برامج أو معدّات ذات تشفير قوي أن تبيع منتجاتها في الخارج. وتقصّدت الشركات الأميركيّة وضع تشفير ضعيف- أعني بذلك أنه قابل للاختراق بسهولة- في منتجاتها المحليّة والدوليّة؛ لأن ذلك أكثر سهولة من الحفاظ على نسختين [إحداهما للداخل بتشفير قوي والأخرى للخارج بتشفير ضعيف] من المنتج عينه.

(*) على الرغم من شيوع استخدام مصطلحي "شبكة الإنترنت" و"الشبكة العنكبوتيّة الدوليّة" بوصفهما شيئاً واحداً، فإن ذلك ليس دقيقاً تماماً. إذ نشأت "العنكبوتيّة" بمبادرة تقنية من خبير المعلوماتيّة السير تيم بارنز لي، الذي ابتكر تقنية ربط النصوص، وتلاها الصور وملفات الصوت وأشرطة الفيديو والمواد كافة، فيما تشمل الإنترنت كل ما يحتويه الفضاء السبراني في الكوابل الضوئيّة لتلك الشبكة، وضمنه "العنكبوتيّة".

وكان العـالم يبـدّل أحوالـه. لم يكن ممكناً إخماد اكتشـافات التشـفير، كما أن العالم الأكاديمـي شرع في الإمسـاك بقدرات تُشـابه مـا تملكه «وكالة الأمـن القومي». في العـام 1993، ألّفـتُ كتـابي الأول التشـفير التطبيقـي (Applied Cryptography) الذي وضع اكتشـافات التشفير في متناول جمهور عام وواسع[1]. كان أمراً كبيراً[2]. وبعـتُ 180 ألف نسـخة من الكتـاب في طبعتين. ووصفته مجلة وايـرد العلميّة بأنّه «الكتـاب الذي تمنّـت «وكالة الأمن القومي» لـو أنّه لم يكتب»؛ لأنّـه يعلّم مهارات التشـفير لغـير المحترفين. جرت البحوث على مسـتوىً عالمـي، وشرعت الشركات الناشـئة غير الأميركيّة في وضع تشـفير قوي في منتجاتها. ووجدَت دراسة جرت في العام 1993، أنّ ما يزيد على 250 من منتجات التشفير كانت تُصنع وتسوّق خارج الولايات المتّحدة[3]. وخشـيت الشركات الأميركيّة من عدم قدرتها على المنافسة في ذلك المجال؛ نظراً للقيود المفروضة على تصدير منتجات بتشفير قوي.

في الوقـت عينـه، بـدأ القلق ينتـاب الـ «إف بي آي» بشـأن قدرة التشـفير القوي عـلى إضعاف قدرتهـا في التنصّت عـلى محادثات المجرمـين. وظهر قلق مماثل بشـأن الـ «إيميل»، لكنه أقل من ذلك المتّصل بصناديق تشفير الصوت التي يمكن وضعها بسـهولة فوق سـمّاعات الهاتف. كانت تلك المرّة الأولى التي اسـتخدم فيها الـ «إف بي آي» عبارة «الدخول في الظلام» لوصف مسـتقبلها المتخيّل في ظل التشـفير فائق القـوّة. كانـت قصـة مرعبة لا تجد مـا يبرّرها، تمامـاً كحالها حـاضراً، لكن المشرّعين صدّقوهـا[4]. وسرعـان ما صاغوا «قانون مسـاعدة الاتّصالات في إنفـاذ القانون»، واختصـاراً «كاليـا»[5]، الـذي تحدّثـت عنه في الفصـل 6؛ ومارس الـ «إف بي آي» ضغوطاً عليهم كي يمرّروا قانوناً يحول دون تصدير منتجات بتشفير قوي، من دون وجود «باب خلفي» فيه، يسمح لـ «إف بي آي» بالدخول منه.

بـدلاً مـن ذلـك، توصّلـت إدارة الرئيـس بيـل كلينتون إلى حـلٍّ: إنّـه الـ «كليبر شـيب» (Clipper Chip). ومثّـل الـ«كليبر شـيب» نظامـاً تقنيّاً للتشـفير، أدمجت في دواخلـه قـدرات الرقابـة التـي طلبتهـا الــ«إف بي آي» و«وكالـة الأمـن القومي».

وزُعِم أن خوارزميّات التشفير كانت قويّة بما يكفي لمنع التنصّت، مع وجود «باب خلفي» يسمح لمن يملك مفتاحه الدخول إلى النص كاملاً. وروّج بوصفه «مفتاح المتعهد»[6]، كما عُدّ تسوية كبيرة تتيح للشركات الأميركيّة المنافسة عالميّاً بتشفيرها القوي، مع الحفاظ على قدرات الـ «إف بي آي» و«وكالة الأمن القومي» في التنصّت.

كانت الأداة الأولى التي احتوت «كليبر شيب»[7] هي الهاتف الآمن الذي صنعته شركة «إيه تي أند تي» (AT&T) الشهيرة في الاتّصالات. لم يكن ذلك هاتفاً خلوياً؛ لأننا كنا لا نزال في 1993. كانت تلك الأداة هي صندوق يوضع بين سماعة الهاتف الخط الأرضي التليفوني، ويعمل على تشفير الصوت. بمعايير تلك الأيام، كان هاتفاً متقناً، مع صوت بنوعيّة مقبولة، لكنه عملي.

ولم يشتره أحد.

برؤية استرجاعيّة، كان شيئاً مكشوفاً. لم يرغب أحد بتشفير مُدمَجٌ فيه «باب خلفي» مفتوح على أذني حكومة الولايات المتّحدة[8]. لم يرغب فيه الأشخاص المعروفون باهتمامهم بأمور الخصوصيّة. لم تُرِدهُ الشركات الأميركيّة. ولم يقبله الناس خارج الولايات المتّحدة، خصوصاً مع وجود بدائل غير أميركيّة تتمتع بتشفير قوي ومن دون «باب خلفي». كانت الحكومة الأميركيّة هي المشتري الوحيد لتلك الأجهزة التي لم تستعمل أبداً[9].

خلال السنوات القليلة التالية، جرّبت الحكومة الأميركيّة مجموعة المبادرات المتّصلة بوجود «مفتاح المتعهد»[10]، وتضمّنت كلها وجود «أبواب خلفيّة» تعطي الحكومة الأميركية القدرة على النفاذ إلى التشفير بأكمله، لكن السوق رفض تلك المبادرات كلها، بتعقّل.

بشّرت هزيمة «كليبر شيب» ومجمل تجربة التشفير مع «مفتاح المتعهد» بنهاية القيود الحكوميّة على التشفير القوي. وتدريجيّاً، رُفِعَت تلك القيود عن برامج الكومبيوتر في 1996، ثم رُفِعَت عن معظم مكوّنات الأجهزة الإلكترونيّة في

السنوات القليلة التالية. ولم يكن توقيت ذلك التغيير متسرّعاً. ففي 1999، كانت السوق العالمية مملوءة بقرابة 800 جهاز فيها تشفير قوي صدّرتها 35 دولة، لم تكن الولايات المتّحدة من بينها[11].

لم يُقض على «كليبر شيب» والقيود على التشفير القوي بأثر من المطالبة باحترام خصوصيّة المستهلك. بالأحرى، قضت عليها المنافسة من الدول الأخرى ومتطلّبات الشركات الصناعيّة الأميركية. لقد تطلّب نمو التجارة الإلكترونيّة وجود التشفير القوي، ولم تستطع «وكالة الأمن القومي» ومكتب الـ «إف بي آي» وقف تطوّره وانتشاره.

رقابة الحكومة تضرّ بالتجارة الأميركيّة

اعتقد كثيرون ممن خاضوا «حروب التشفير»، وفق تسمية كانت رائجة أنهم انتصروا في تسعينيات القرن العشرين[12]. في المقابل، أظهرت وثائق سنودن أن مفهوم زرع «باب خلفي» تنفذ الحكومة الأميركيّة منه إلى الشيفرة بأكملها، استمر العمل به بصورة سريّة من قبَل «وكالة الأمن القومي» والـ «إف بي آي». ولأن سنودن أذاع الأمر على الملأ، شرعت الشركات الأميركيّة في خسارة زبائنها في الخارج؛ لأن الآخرين لا يرغبون في رؤية معلوماتهم وبياناتهم متجمعة في يد الحكومة الأميركيّة.

وتلحق الرقابة التي تمارسها «وكالة الأمن القومي» خسائر بالتجارة الأميركيّة بواسطة ثلاث طرق مختلفة[13]. إذ بات الناس ينفرون من «سُحُب المعلومات» الأميركيّة، وهناك انخفاض في مبيعات الحواسيب ومعدّات التشبيك الأميركيّة، وأخيراً لم يعد أحد يثق بالشركات الأميركيّة.

في 2013، تكشّفت حقيقة أن «وكالة الأمن القومي» تحصل بواسطة برنامج «بريزم» (PRISM)، على بيانات الجمهور من الشركات الأميركيّة لخدمات «حوسبة

السحاب»؛ وارتدّ الأمر بشدّة على العلاقات العامة للشركات الأميركيّة[14]. وبصورة شبه فوريّة، ظهرت مقالات تتحدّث عن خسائر في السوق تسجّلها الشركات الأميركيّة العاملة في «حوسبة السحاب» وشريكاتها، لمصلحة الشركات الآتية من بلدان ينظر إليها بوصفها محايدة، كسويسرا[15]. في العام 2014، أظهر مسح استطلاعي عن الشركات الكنديّة والبريطانيّة أن 25 ٪ منها شرعت في نقل مخازن معلوماتها خارج الولايات المتّحدة، حتى لو أدى ذلك إلى انخفاض مستواها التقني[16]. وبينّ مسح آخر أنّ الكشوفات عن «وكالة الأمن القومي» أقلقت المدراء التنفيذيّين بشأن بياناتهم وتخزينها[17].

تتفاوت التقديرات بشأن خسائر الشركات الأميركيّة التي تقدّم خدمات «حوسبة السحاب»[18]. وتوقّعت دراسة أجرتها «مؤسّسة الابتكار وتقنيّة المعلومات» (Information Technology & Innovation Foundation) في العام 2013، خسارة في العائدات تتراوح بين 22 و35 بليون دولار في السنوات الثلاث التالية؛ ما يمثّل نسبة تتراوح بين 10 ٪ و20 ٪ مما تحصل عليه شركات «حوسبة السحاب» الأميركيّة من أعمالها خارج بلادها. وتعتقد شركة «فورستر ريسيرش» (Forrester Research) للتحليلات بأن تلك الأرقام منخفضة، إذ تقدر الخسائر بقرابة 180 بليون دولار؛ لأن بعض الشركات الأميركيّة ستنتقل إلى مقدّمي «حوسبة السحاب» في الخارج[19].

وفي ذلك المجال عينه، عانت شركات الكومبيوتر والإنترنت الأميركيّة ضربات موجعة أيضاً. وفي 2013، أعلنت شركة «سيسكو سيستمز» المختصّة في الشبكات الرقميّة أنها سجّلت رابع خسارة فصليّة متتاليّة وتراوحت بين 8 ٪ و10 ٪[20]. كذلك سجّلت شركة «إيه تي أند تي» للاتّصالات خسائر في عائداتها، معلنة أنها تواجه مشكلات في خطط توسّعها في السوق الأوروبي[21]. وهناك خسائر لشركة «آي بي أم» في الصين[22]، وهو ما ينطبق على حال شركة «كوالكوم» (Qualcomm) الأميركيّة العاملة في صناعة الحواسيب المتنوّعة[23]. وخسرت شركة «فيريزون»

الأميركيّـة المختصـة في التجارة الإلكترونيّـة عقداً ضخماً مع الحكومـة الألمانيّة[24]. هنـاك مزيـد من ذلك السـيل[25]. حـضرت بنفـسي اجتماعات خاصة شـكت فيها شركات برامـج الكومبيوتـر الأميركيّـة من خسـائر ضخمـة في مبيعاتهـا الخارجيّة. وكتب جون شـامبرز، المدير التنفيذي لـ «سيسكوسيسـتمز» إلى إدارة الرئيس باراك أوباما، شاكياً من أنّ اختراق «وكالة الأمن القومي» للمعدات الإلكترونيّة الأميركيّة «من شـأنه نسـف الثقة بصناعتنا وقدرة شركات التكنولوجيـا الأميركيّة على تقديم منتجات تصلح للسوق العالميّة»[26].

وتردّد شـكوى شـامبرز أصـداء الطريقة الثالثـة للضرر الذي حـاق بالشركات الأميركيّة جراء كشـوفات سـنودن عن رقابـة «وكالة الأمن القومـي»؛ وهي فقدان الثقـة. إذ بـات العالم يعـرف أنّ الـشركات الأميركيّة تعطي «وكالـة الأمن القومي» منفـذاً إلى الهياكل الرئيسـة للإنترنـت، والشركات العاملة في «حوسـبة السـحاب» تعطـي الوكالة منفذاً لحسـابات مسـتخدميها. وبـات العالم يعرف أيضـاً أن «وكالة الأمن القومي» تقتحم معدّات الكومبيوترات الأميركيّة عند تصديرها، وتدسّ فيها خلسـة مُكوّنات تخدم الرقابة التي تمارسـها الوكالة[27]. وصـار العالم على دراية بأنّ محكمـة سريّة ترغِـم الشركات الأميركيّة عـلى التجاوب مع متطلّبـات رقابة «وكالة الأمـن القومـي»، ثـم تأمرها بأن تكـذب على الجمهور في ذلك الشـأن. هـل لنا أن نستعيد قصة «لافابِت» في الفصل 5 في هذا الكتاب؟

تفاقمـت معضلة انعدام الثقة مع التطمينات المتوالية من إدارة الرئيس أوباما بأن «وكالـة الأمن القومي» ركّزت معظم جهودها على غـير الأميركيّين. إذ يأتي ما يزيد على نصف عائدات شركات «حوسـبة السحاب» الأميركيّة من الأسواق الخارجيّة. وعـبرّ عن ذلك المأزق مؤسّـس «فيسـبوك» مـارك زوكربـرغ، أثناء مقابلـة في العام 2013، بأفضـل الكلـمات قائـلاً: «تمثّل ردّ الحكومـة الأميركيّة بالقـول «لا تقلقوا، لم نكن نتجسّـس على الأميركيّين». يا للروعة. كم تسـاعد تلـك الكلمات الشركات

التي تسعى إلى لتعامل مع الناس في أصقاع العالم قاطبة، وكم توحي بالثقة بشركات الإنترنت الأميركيّة»[28].

وإنصافاً، يجدر القول إن ذلك المأزق ربما كان مجرد مشهد عابر نجم من كثافة التغطية الإعلاميّة للرقابة التي مارستها «وكالة الأمن القومي»، ولا نعلم إلى متى سيستمر. نعلم أنّ بلداناً كثيرة- وألمانيا بلد كبير أيضاً- باتت تحاول صنع «سحابة معلومات» محليّة؛ بهدف الحفاظ على بياناتها الوطنيّة بعيداً عن أيدي الوكالة[29]. وأخيراً، أصدرت المحاكم الألمانيّة أحكاماً ضد ممارسات «غوغل»[30] و«فيسبوك»[31] و«آبل»[32] في جمع البيانات؛ كذلك ناقشت الحكومة الألمانيّة حظر كل الشركات الأميركيّة التي تتعامل مع «وكالة الأمن القومي»[33]. وتتجه خصوصيّة البيانات لرسم شكل السلامة العامة الجديدة في التجارة الدولية[34].

وكذلك تشكّل الخصوصيّة شرطاً تعاقديّاً جديداً. وباطّراد، صارت الشركات الأميركيّة الكبرى تشترط على مقدّمي خدمات تقنية المعلومات لها أن يوقّعوا عقوداً تضمن عدم وجود «أبواب خلفيّة» في النُظُم المعلوماتيّة التي يبيعونها للشركات. وبتحديد دقيق، تعمل اللغة التعاقديّة على إلزام أولئك الباعة بألاّ تتضمّن نُظُمهم شيئاً يسمح لطرف ثالث بالوصول إلى معلومات الشركات وبياناتها. وبذا، يصبح من الصعب على الشركات البائعة للنُظُم المعلوماتيّة التعاون مستقبلاً مع «وكالة الأمن القومي» أو وكالات حكوميّة أخرى؛ لأن ذلك يعرّضها إلى مسؤولية قانونيّة بموجب العقود الموقّعة مع زبائنها من الشركات الكبرى. وفي حال لم يوقّعوا تلك العقود وشروطها، فلسوف يخسرونها لمصلحة شركات تقبل التوقيع على تلك الشروط.

ومن الصعب علينا أيضاً معرفة مدى ارتفاع حدّة المنافسة مع منتجات وخدمات تُصنَع في دول أخرى[35]. إذ تتقدّم شركات عدّة في أوروبا وآسيا وأميركا الجنوبيّة، للاستفادة من أجواء الحذر المستجدّة[36]. واستناداً إلى التجربة

مع «حروب الخصوصيّة» في تسعينيات القرن العشرين، هناك احتمال أن تقدّم مئات من الشركات غير الأميركيّة منتجات في المعلوماتيّة لا تطالها القوانين الأميركيّة[37]. ويشمل ذلك البرمجيات الرقميّة، خدمات «حوسبة السحاب»، مواقع شبكات التواصل الاجتماعي، معدّات الشبكات الإلكترونيّة، و... كل شيء آخر. وبغض النظر عن مدى مأمونيّة تلك المنتجات- لأن هناك بلداناً أخرى ربما وضعت «أبواباً خلفيّة» لها في المعدّات التي تستطيع السيطرة عليها- أو حتى مدى كونها فعليّاً خارج قدرة «وكالة الأمن القومي» في النفاذ إليها؛ فلا ريب أن رقابة الوكالة ألحقت ضرراً هائلاً بالتجارة والأعمال الأميركيّة.

تكلفة رقابة الشركات على التجارة

في زمن سابق، ساد ما يشبه التسليم بمقولة أن لا أحد يدفع ثمن الخصوصيّة. ولفترة ما، كانت المقولة صحيحة لكن السلوكيّات أخذت تتغيّر.

إذ بات الناس أكثر دراية بمن يستطيع النفاذ إلى بياناتهم ومعلوماتهم، وبرزت مؤشّرات عن استعداد بعض الناس في السنوات الأخيرة لأن يدفع مقابل الحفاظ على الخصوصيّة. في العام 2000، أظهرت دراسة[38] أنّ الإنفاق بواسطة الإنترنت سوف يزيد بقرابة 6 بلايين دولار سنويّاً، إذا أحس الناس أنهم محميّون جيّداً أثناء عمليات الشراء[39]. وفي 2007، خلصت دراسة إلى القول إنّ جمهور المستهلكين لديه استعداد لأن يدفع 60 سنتاً لكل سلعة ثمنها 15 دولاراً، مقابل الحصول على حماية لخصوصيّته أثناء عمليات الشراء على الإنترنت. وبعد ما كشفته وثائق سنودن، تنشر شركات كثيرة إعلانات عن الحماية من الرقابة الحكوميّة.

ولا تقدّم معظم الشركات الخصوصيّة كملمح تفضيلي لها في السوق، لكن هناك بعض الاستثناءات[40]. إذ يتميّز محرّك البحث «داك داك غو» (DuckDuck Go) بأن نموذجه في العمل يستند إلى عدم تتبّع مستخدميه[41]. وتقدّم شركة «ويكَر» (Wickr) برنامجاً رقميّاً لتشفير التراسل الفوري يشمل الصورة وأشرطة الفيديو

والرسـائل النصيّـة للخلوي والبريـد الإلكـتروني، ومحادثات الإنترنـت، والملفات المرفقة بالرسـائل وغيرها. ويقـدّم موقع «إيلو» (Ello) منصـة للتواصل الاجتماعي لا تتتبـع مسـتخدميها[42]. لا تتمتـع تلـك الـشركات بالقوة والصيـت الذي تملكه الشركات الراسخة في تلك الحقول، لكنها تتقدّم في أعمالها باطّراد.

إذاً، نحـن نشـهد صعـوداً لأهمية الحفـاظ على خصوصيّـة المسـتهلك والزبون، بالتزايـد المطّـرد في عـدد الشركات التي اسـتحدثت منصـب «مديـر الخصوصيّة». ويُعرّف الأخير بأنه مدير تنفيذي يتولى المسـؤولية عن المخاطر في السـمعة والقانون المتّصلـة بالمعلومـات والبيانـات التـي تحوزها الشركـة. وبات لمديـري الخصوصيّة منظّمـة خاصة بهم تسـمّى «رابطـة محـترفي الخصوصيّـة» (Association of Privacy Proffessionals)، وشرعوا في إرساء قوانين وقواعد تنظيميّة، حتى مع غياب الدعم الحكومي لهم. وينهضون بتلك الأمور لأنها تشكّل تجارة مجزية.

10
الخصوصيّة

لعل المفهوم المغلوط الأكثر شيوعاً عن الخصوصيّة أنها تتعلّق بإخفاء أمر ما[1]. ثمة عبارة شائعة تقول: «إن لم ترتكب خطأ، فليس لديك ما تخفيه»، موحيَةً بأن الخصوصيّة لا تنقذ سوى من يرتكبون أفعالاً مغلوطة.

وبقليل من التفكّر، يتبيّن أنّها عبارة لا معنى لها[2]. ليس خطأً ممارسة الجنس، أو الاغتسال في الحمّام أو الغناء تحت «الدوش». ليس خطأً أن نبحث عن وظيفة من دون أن نعلِم رب عملنا الراهن. ليس خطأً البحث عن أمكنة تؤمن خصوصيّتنا أثناء التأمّل أو التحدّث عن أمور عاطفيّة أو شخصيّة؛ وكذلك الحال عندما نضع رسائلنا في مغلّفات خاصة، ونمنح ثقتنا لصديق بعينه دون سواه.

أبعد من ذلك، حتى قائلي تلك العبارة لا يؤمنون بها فعليّاً. في مقابلة جرت سنة 2009، صاغ المدير التنفيذي لـ «غوغل» إريك شميدت الأمر على النحو التالي: «إذا كان لديك ما لا تريد أي شخص آخر أن يعرفه، فلربما يجب عليك في المقام الأول ألا تفعل ذلك»[3]. ولكن، في العام 2005، منع شميدت موظّفي «غوغل» من التحدّث إلى مراسِلي موقع «سي نِت» الإعلامي؛ لأن أحد المراسلين كشف تفاصيل شخصيّة عن شميدت في أحد المقالات[4]. وفي العام 2010، صرّح مؤسّس «فيسبوك» مارك زوكربرغ بأنّ الخصوصيّة لم تعد «عُرفاً اجتماعيّاً»[5]، لكنه اشترى أربعة منازل قريبة من مسكنه في «بالو آلتو» كي يؤمّن خصوصيّته[6].

هنـاك القليل مـن الأسرار التي لا نخبر عنها *أحداً*، ونبقى على ثقة بأن شـيئا من السريّـة يحـوط بها حتى بعـد أن نخبر عنها *أحداً* مـا بعينه[7]. وكذلك ندبّج رسـائل حميميّة للأصدقاء والمحبّين، ونبوح للطبيب بأشـياء لا نخبرها سـواه، ونقول أشياء في اجتماعات العمل لا نعلنها على الملأ. ونتّخذ أسماء مستعارة للتمييز بين شخصيتنا في العمل وشـخصيتنا الفعليّة، وكذلك الحال عندمـا نريد تجربة شيء جديد بطريقة مأمونة[8].

أظهر مـارك زوكربرغ، المدير التنفيذي لـ «فيسـبوك»، سـطحيّة لافتة حين قال: «تملك هويّة وحيدة. الأرجح أنّ الزمن الذي كنت تقدّم فيه صورة عنك للأصدقاء والزمـلاء في العمـل تختلف عن تلـك التي تقدّمها لبقية الناس، أصبح موشـكاً على الانتهاء. فمجرد امتلاكك لهويّتين يعطي نموذجاً عن عدم المصداقيّة»[9].

لسـنا الشخص نفسـه بالنسبة لكل شـخص نعرفه أو نصادفه. ونتصرّف بطريقة مختلفة مع أصدقائنا وعائلاتنا وزملائنا في العمل وما إلى ذلك. نأكل في المطعم بطريقة تختلـف عـن المنزل. نروي قصصاً لأطفالنا تختلف عما نحكيه لمن نلتقيه في جلسـات الـشرب. ليـس بالضرورة أننا نكذب، على الرغم من أننا نفعل ذلك أحياناً؛ لكننا لا نكشف عن المناحي نفسها من ذواتنا للناس كافة. ذلك شيء إنساني أصيل. تتيح لنا الخصوصيّـة أن نتصرف بطرق تتناسـب مع الظروف المختلفـة التي قد نواجهها. في ظـل خصوصيّة المنزل وغرفة النوم، نسـترخي بطريقة تختلف كليّاً عما نكونه بوجود آخرين.

إنّ الخصوصيّـة حـقٌّ إنسـاني أصيـل، وهو شرط لاسـتمرارية الشرط الإنسـاني بكرامـة واحـترام[10]. إنّه حقّ يتّصل بمسـألة الاختيار وامتلاك مـا يكفي من القوة للتحكّـم بالطريقـة التـي تقدّم بها نفسـك إلى العـالم. وتفضّل دانا بويـد المختصّة في الثقافات الإثنيّة على الإنترنت، صوغ المسألة على النحو التالي: «لا تتعلّق الخصوصيّة

بوجـود ما يقوم بوكالة ما عنك، بـل إنّ القدرة على تحقيق الخصوصيّة هي تعبير عن وجود الوكالة»[11].

عندمـا نفقد الخصوصيّة، نفقـد قدرتنا عـلى التحكّم بطريقة تقديم أنفسـنا[12]. نفقـد تلـك القـدرة عندما تتشـارك بالصدفة مجموعة ما على «فيسـبوك» أقـوالاً لنا، مـع مجموعة أخـرى، وكذلك نفقـد تلك القدرة كليّـاً عندما تجمع الحكومـة بياناتنا ومعلوماتنا. وحينها، نسـأل أنفسنا «كيف عرفت الحكومة بالأمر»؟ كيف تأتّى أنني فقدت التحكّم في من يجدر به أن يعرف عن طفولتي المعذّبة، أو بالسـخريّة الهاذرة، أو قضائي العطلة في جمهورية الدومنيكان؟ ربما تعرف ذلك الشـعور جيّداً[13]: ربما أحسسـت به عندما انضمت أمّك إلى قائمة أصدقائك على «فيسـبوك» أو أي شـبكة اجتماعيّـة تعدّها حيزاً لك ولأصدقائك. الاعتداءات على الخصوصيّة هي انتهاكات تقتحم حياتنا[14].

ثمة أسـاس فيزيولوجي للخصوصيّة[15]. إذ يشدّد بيتر واتس، وهو اختصاصي في البيولوجيـا، عـلى أن الرغبة في الخصوصيّة أمر أصيل وليس مكتسـباً؛ مشـيراً إلى أن الحيوانـات اللبونـة تضحي أقل تجاوبـاً في ظل وجود رقابة. نعتـبر الرقابة تهديداً ماديّـاً وجسـديّاً؛ لأن الحيوانـات في عـوالم الطبيعـة تُراقَـب مـن قِبَل من يسـعى إلى افتراسـها. تجعلنا الرقابة نحـّس كأننا فرائس، تماماً مثلما تجعل مـن يراقبنا يتصرّفون كمفترسين[16].

كتب الفلاسـفة والروائيون وعلماء النفس والاجتماع والمختصّون بالتقنيّات عن تأثير الرقابة الدائمة، بل حتى مجرد وجود انطباع بالرقابة الدائمة. وبيّنت الدراسات أيضـاً أننـا نكـون حينها أقـل تمتّعاً بالصحة جسـديّاً ونفسـيّاً[17]. وتتملكنا مشـاعر الكآبـة والتوتر وتضاؤل القيمة الذاتيّـة. تجرّدنا الرقابة من كرامتنا[18]. وتهدّد ذاوتنا كأفراد[19]. في سـجون العالم ومعتقلاته كافة، تسـتعمل الرقابة الدائمة أداة تكتيكيّة لسلخ الفرد عن إنسانيته.

ليست الاعتداءات على الخصوصيّة بمتساوية؛ ذلك أنّ السياق التي تحصل فيها يصنع الفارق بين بعضها بعضاً. هناك فارق بين أن يعثر ضابط في «أمن إدارة النقل» على مواد إباحيّة في حقيبتك، وبين أن تعثر عليها زوجتك. ثمة فارق بين معرفة الشرطة بأمر تعاطيك بعض المواد، وبين معرفة أصدقائك بذلك الأمر. وكذلك لا تتساوى الأضرار الناجمة عن الاعتداءات على الخصوصيّة. إذ تكون أشد تأثيراً في من يعيش في الهوامش الاجتماعيّة- الاقتصادية، ومن ينتمون إلى مجموعات مهمّشة عرقيّاً وسياسيّاً وإثنيّاً ودينيّاً. وكذلك حال من يشغلون مناصب مهمّة ويكونون عرضة لاستمرار موافقة الناس على ما يفعلون. إنّ حياة بعضنا تعتمد كليّاً على الخصوصيّة.

وباتت خصوصيّتنا عرضة للغزو من الرقابة الدائمة. وأصبح ضروريّاً فهم كيفيّة حدوث ذلك الغزو كشرط لفهم الرهانات المتّصلة به.

الزائل

على مرّ التاريخ، اتّسمت محادثاتنا وتفاعلاتنا مع بعضنا بعضاً بطابع الزوال. إنّها الطريقة التي نفكّر بها عادة بالمحادثة. كانت الاستثناءات عن تلك القاعدة نادرة إلى حدّ أنها تستحق التسجيل: مفكّرة محفوظة، كاتب يدون بطريقة الاختزال وثائق عن مجريات المحكمة، مرشّح سياسي يصنع خطاباً مسجّلاً.

تغيّر ذلك تماماً. صارت الشركات تجري عدداً أقل من المقابلات الشخصيّة المباشرة. ويتواصل الأصدقاء مع بعضهم بعضاً بواسطة الإنترنت. خضّت وزوجتي محادثات حميمة برسائل الخلوي النصيّة. نتصرف جميعنا كأن تلك المحادثات زائلة، لكنها لم تعد كذلك. إذ باتت تخزّن بطرق لا نملك أي سيطرة عليها.

يصعب التخلّص من المحادثات المدوّنة. تلقى الجنرال أوليفر نورث ذلك الدرس مبكّراً في العام 1987 [20]. إذ تبيّن له أن الرسائل التي ظّن أنّه حذفها منها،

كانت محفوظة في نظام إلكتروني خاص بالموظّفين الكبار في البيت الأبيض، ما يمكن اعتباره شكلاً أولياً من البريد الإلكتروني. وبعد عشر سنوات، تعلّم بيل غيتس الدرس نفسه، عندما قُدّمَت محادثاته بواسطة البريد الإلكتروني إلى القضاء كجزء من التحقيق في الدعوى التي رُفِعَت بشأن احتكاريّة «مايكروسوفت»[21]. وتلقّى 100 نجم ونجمة الدرس نفسه في العام 2014، عندما سُرِقت صور شخصيّة حميمة لهم- بعضها كان يعدُّ محذوفاً- من سحابة رقميّة لشركة «آبل» تحمل اسم «آي كلاود» (iCloud)، وجرى تشاركها على نطاق أوسع كثيراً مما قصد أصحابها بشأنها[22].

صار الزوال شأناً فائق الصعوبة. لا يزال معظم المحادثات الشفويّة خارج التسجيل، لكن إلى متى سيستمر ذلك؟ في متاجر البيع بالتجزئة، يسجّل نظام رقمي للمراقبة وجودنا، حتى لو لم نفعل سوى تقليب المعروضات، وحتى لو دفعنا كل مشترياتنا نقداً. تسجّل بعض البارات أرقام البطاقة الشخصيّة لكل من يدخلها[23]. وعلى الطائرة، لم يعد مستطاعاً شراء زجاجة نبيذ إلا ببطاقة الائتمان. ولسوف يزداد الأمر سوءاً مع استمرار الميل إلى التسجيل الواسع لمناحي الحياة كافة.

وصف كاتب الخيال العلمي تشارلز ستروس ذلك الأمر بأنه نهاية ما قبل التاريخ[24]. لن ننسى شيئاً لأننا سنقدر دوماً على استرجاعه من الذاكرة الرقميّة لحاسوب ما[25]. إنّه لأمر مستجدّ على النوع البشري برمّته، ولسوف يكون كنزاً لمؤرّخي المستقبل، وللأفراد المعاصرين ممن يسعون إلى الحصول على بيانات أفضل من أجل التأمّل والتقييم الذاتي.

سوف تغير القدرة على تدوين كل شيء بما يجعله متوافراً إلى الأبد الأفراد والمجتمعات معاً[26]. ليست ذاكراتنا ولا انطباعاتنا بمثل الثبات الذي نتوقّعه. ثمة ما لا نلاحظه، حتى بعض الأشياء المهمّة. ونتذكر أشياء كثيرة بطريقة مغلوطة، حتى إننا لا نكون متأكّدين من استعادته بصواب[27]. كذلك ننسى أشياء مهمة كنّا

نعتقـد أننا لن ننسـاها أبـداً. من يدأب على الكتابـة في مفكّرته يعـرف تلك الظاهرة جيّـداً، وهـي أن مـا كتبناه قديماً يبـدو كأنه كتب بأيـد أخرى. أنا أيضـاً لاحظتُ أن الاحتفاظ برسائلي الإلكترونيّة كلها طيلة عشرين سنة، تصنع فارقاً كبيراً في تفكيري عن تاريخي الشخصي.

يملك ربع البالغين الأميركيّين سـجلات جرميّة. حتى المخالفات البسـيطة ربما لاحقـت النـاس طيلة حياتهم مخلّفـة آثاراً واسـعة عليها[28]- لذلك السـبب، تلجأ بعض الحكومات إلى محو السـجلات الإجراميّة بعد مرور زمن معين عليها. ويعني فقدان الزائل أنّ كل ما تقوله وتفعله يبقى يلاحقك إلى آخر العمر[29].

يمثّـل إجـراء محادثات تتلاشـى بمجرد حدوثهـا عُرفـاً اجتماعيّاً يتيـح لنا راحة واسـترخاء كبيريـن، وأن نقول أشـياء ما كُنّـا لنقولها بحضور جهاز تسـجيل. وعلى مدى أبعد، يشـكّل النسيان- والخطأ في التذكّر- ركناً في تعاملنا مع تاريخنا. إذ يمثّل النسـيان مسـاعداً قويّاً للغفران. إذ تبهت الذاكرة الفرديّة والجماعيّة، فيصبح الماضي أقـل حدّة؛ ما يسـمح لنـا بغفران الإسـاءات الماضيـة. يصعب إقناعي بـأن زواجي سيكون أفضل لو جرى الاحتفاظ بسجل تفصيلي عن المشاجرات والنقاشات كلها. يـؤدي فقدان الزائـل إلى تغيير اجتماعي ونفسي هائل، وهو ليـس من النوع الذي لا يبدو أن مجتمعنا مستعد له.

الرقابة بالخوارزميّات

تتمثّـل إحـدى الحجـج الأكثـر شـيوعاً بشـأن الرقابـة الجماعيّـة في القـول إنّهـا تجـري بموجـب جـداول الرياضيّـات الحاسـوبيّة، وتسـمّى تقنيّـاً «خوارزميّـات» (Algorithms)، وليـس وفقـاً للأشـخاص، مـا يعنـي أنهـا لا تنتهـك خصوصيّات الناس. ما ذلك إلا بهتان صريح[30].

هناك فارق مهمٌّ في السياسة بين رقابتي البشر والحاسوب. ومنذ أن أمدّ سنودن الصحافة بخزّان من الوثائق فائقة السريّة، أضحى الناس على دراية بتلاعب «وكالة الأمن القومي» بالكلمات[31]. إذ تملك كلمة «جمع» تعريفاً محدّداً في وزارة الدفاع الأميركيّة[32]. إنّها لا تعني جمعاً؛ بل تفيد بأن هناك شخصاً ينظر في تلك البيانات ويحلّل تلك المعلومات[33]. في العام 2013، شبّه جايمس كلايبر، رئيس «الاستخبارات القوميّة»، خزّان المعلومات في «وكالة الأمن القومي» بالمكتبة. «الكتب كلّها مخزّنة على الرفوف، لكن قلّة منها تُقرأ فعليّاً[34]. إذاً، تتمثّل مهمّتنا المتصلة بالحفاظ على الأمن والحريات المدنيّة والخصوصيّة، في أن نكون على أقصى درجات الدقّة عندما نذهب إلى تلك المكتبة ونبحث عن الكتب التي نرغب في قراءتها فعليّاً».

فكّر في صديق لك يملك آلافاً من الكتب في منزله. وفق كلايبر، لا يملك ذلك الصديق سوى الكتب التي قرأها فعليّاً!

وللسبب عينه، يصرّ كلايبر على أنّه لم يكذب أثناء مثوله للجنة استماع في مجلس الشيوخ[35]، عندما أجاب بـ «كلا» عن سؤال: «هل تجمع «وكالة الأمن القومي» أي نوع من البيانات عن ملايين أو عشرات ملايين الأميركيّين»؟ من وجهة نظر الجيش، لا يشكّل الأمر رقابة إلا إذا نظر شخص ما إلى البيانات وقرأ المعلومات، حتى لو كانت الجداول الخوارزميّة التي طوّرتها وزارة الدفاع والشركات المتعاقدة معها، قد حلّلتها المرّة تلو المرّة.

ليست تلك المرّة الأولى التي تُرَدّد فيها تلك الحجة. إذ إنّها مثّلت ركناً أساسيّاً في دفاع «غوغل» عن صنعه إعلانات يجري توجيهها بموجب مضامين لها طابع حسّاس وشخصي، في الأيام الأولى لظهور البريد الإلكتروني «جي ميل». إذ تنظر الأجهزة الذكيّة التي تملكها شركة «غوغل» في البريد الشخصي للأفراد، ثم تُدخِل إعلانات تتناسب مع مضمون كل بريد على حدة، في ذيل الرسائل. ولكن، لا يقرأ

أشـخاص رسائل ذلك البريد، بل ينهض الحاسـوب وحده بتلك المهمة[36]. ووفق ما أسرّ به لي شـخصياً أحد مسـؤولي «غوغل» أثناء الأيام الأولى لإنشاء «جي ميل»، «يشبه القلق بشأن قراءة الكومبيوتر لبريدك أن تحسّ بالقلق لأن كلبك رآك عارياً».

لكن ذلك ليس صحيحاً، بل إن مَثَل الكلب يدحضه تماماً. عندما يشاهدك كلب عارياً، لا ينتابك القلق بسبب ثلاثة أمور رئيسة: إذ لا يستطيع الكلب أن يفهم ويعي ذلك المشهد، مثلما يفعل أي شخص. ولا يؤسّس الكلب قرارات مستقبليّة أو يصنع ذكريات عن ذلك المشهد، ليس بالطريقة التي تحدث عند البشر. ولا يستطيع الكلب أن يخبر شخصاً أو حتى كلباً، عن مشاهدته لك عارياً.

وعندمـا يراقبـك كومبيوتـر، تنتفـي أسـس المقارنـة مـع الكلـب. إذ يسـتطيع الكومبيوتر أن يتعامل بذكاء مع ما يشـاهده، كما يؤسّـس قراراته على ذلك. ربما قيل لـك إن الكومبيوتـر لا يختـزن معلومات عنك، لكـن لا أحد يقـدّم لـك برهاناً على ذلك[37]. ولربما قيل لك أيضاً إنّ الكومبيوتر لن يلفت نظر أي شخص إذا تقاطعت بياناتـه ومعلوماته عنك بطريقة «مثيرة للاهتـمام»، لكن لا أحد يقدّم لك تأكيداً عن ذلـك. وليس مـن طريقة للتثبت من أن شـخصاً لن يطّلع ويتفهـم الخلاصات التي صاغها الكومبيوتر بشـأنك، وأن لا أحد سيسـتخدم بيانات الكومبيوتر في ممارسـة تمييز ضدك أو إصدار أحكام بشأنك، بالاستناد إلى مشاهدات الكومبيوتر عنك.

أبعـد مـن ذلـك، عندما يخـزّن الكومبيوتـر، يحضر دومـاً خطر الانكشـاف. من الممكـن أن تتغـيّر قوانين الخصوصيّة في أي وقـت، فتتيح اسـتعمال بياناتك القديمة مـن دون موافقتك الصريحة. كذلك ثمة احتمال أن يحدث اختراق وسـطو للبيانات من الـ «هاكرز» أو تنظيمات إجراميّة. وتسـتطيع المنظّمة التي تحصل على بياناتك أن تسـتخدمها بطرق جديدة مع كشـفها للعلـن، أو تبيعها لمنظّمات أخرى. ويسـتطيع الـ «إف بي آي» أن يرسـل مذكرة أمن قومي إلى من يملك بياناتك، فيحصل عليها.

مـن ناحية أخرى، لا تسـتطيع أي محكمـة على وجـه الأرض أن تحصل على وصف لمشهدك عارياً من الكلب الذي شاهدك حينها.

يكمـن الفـارق الرئيـس بـين الكلـب والكومبيوتـر في أن الكلـب لا يسـتطيع التواصل مع أشـخاص آخرين بشـأن إيصـال البيانات والمعلومـات عنك، بطريقة تكـون مجدية إلى حدّ يثير قلقك[38]. إذ يكتب بشرٌ الجداول الخوارزميّة للكومبيوتر، وكذلـك يجري بشرٌ تحليلاً لنتائج تلك الجداول. وعندما نفكر في رقابة خوارزميّات الكومبيوتر المفروضة علينا، وما تعطيه من قدرة على تحليل معلوماتنا، يجدر أن نفكر بالأشـخاص الذين يقفون خلف تلك الخوارزميـات. إذ تصبح تلك الخوارزميات رقابـة إذا دقّـق أشـخاص بها، إضافـة إلى حقيقتين هما أنهم يسـتطيعون ذلك، وأنّهم يوجّهون الخوارزميات بما يجعلها رقابة.

أنت تعرف جيّداً أن تلك الأمور صحيحة. إذا اعتقدت أن كلايبر محق في كلامه عـن الكومبيوتـر والكلب، فلن تعـترض على وضع كاميرا للرقابـة في غرفة نومك، طالما أن هنالك قوانين تتحكّم بقدرة الشرطة على التدقيق بها.

كذلـك لـن تعترض عـلى إجبارك عـلى ارتداء جهـاز إلكتروني يبـث إلى جهات حكوميّة كل ما تقوله على مدار الساعة، طالما أنّ الموظفين الحكوميّين الذين يلتقطون ذلك البث يلتزمون بقوانين تضبط عملهم. في المقابل، إذا كنت تعترض على الأمور السـابقة[39]، فذلـك يرجـع إلى إدراكك أن خصوصيّتك تتأذى مـن الجمع المؤتمت للمعلومات والبيانات، وعمليات تحليلها بواسـطة خوارزميات الكومبيوتر، بغض النظر عن موقع العنصر البشري في تلك العمليات.

تحديد الهويّة وإغفالها

مررنـا جميعـاً بتجربة التعريف عن أنفسـنا عـلى الإنترنت. وتربـط بعض مواقع الإنترنت هويتك الفعليّة مع هويّتك الشبكيّة، كمواقع البنوك والمؤسّسات الحكوميّة

وغيرهـا. ويربط بعضها هويّتك الشبكيّة مع نظام للدفع- غالباً ببطاقة الائتمان-، وبعضها الآخر يربط تلك الهويّة مع حسـابك البنكي أو هاتفك الخلوي. ولا تبدي بعـض المواقـع اهتماماً بهويّتك الفعليّة، فتتيح لك أن تسـتخدم اسـماً مميّـزاً فيها. ثمة كثير من المواقع التي تستطيع أن تعمـل بتلك الطريقة. ومثلاً، مـن الممكن تصميم مخـزن «آي تيونز» التابع لشركة «آبل» بطريقة لا تتضمّن معرفته هويّتك فعليّاً لمجرد منحك القدرة على الوصول إلى بعض ملفات الموسيقى والفيديو.

تشـمل طـرق التعريـف بالهويّـة والتثبّـت مـن أصالتهـا، اسـتعمال كلـمات المـرور، والقياسـات البيولوجيّـة التـي تعرف باسـم «بيومتريكـس» (Biometrics) والتـذكارات[40]. كنـتُ مـن بـين الذين كتبوا بتوسّـع عن نُظُـم التعـرّف إلى الهويّة والتثبّـت منهـا، والمقارنـة بينهـا في القـوّة ونقـاط الضعـف. ومـن دون الخوض في التفاصيـل، تتمثّـل الخلاصـة في أن لا نظامَ كامـل، لكنها بعمومها جيّـدة في أداء ما أعدّت من أجله. وبصورة أساسيّة، تعمل نظم التثبّت من الهويّة بكفاءة.

وترجـع تلك الكفاءة إلى أن مسـتخدمي تلك النُظُم يطلبون بأنفسـهم أن يجري التثبت من هويّتهم. عندما تسـتخدم بريـد «هوت ميل» الإلكتروني، فأنت تريده أن يقتنع بأن ما تسـتعمله هو حسـابك فعليّاً، كما تريد إقناع البنك بأن تلك هي نقودك. في المقابـل، ربـما لا ترغـب في أن تربـط شركـة «إيه تي أنـد تي» هويّتك مـع زياراتك لمواقـع الإنترنـت كافة التـي تجريها بهاتفك الذكـي؛ لكنك ترغـب في أن تحوّل تلك الشركة مكالماتك كافة إلى ذلك الهاتف. تحاول تلك النُظُم كلها أن تجيب عن سـؤال هو: «هل ذلك الفرد هو الشـخص الذي يزعمه فعليّاً»؟ ولذا يكون من السهل جمع البيانات عنا من شـبكة الإنترنت، بمعنـى أن معظمها يأتي من مصادر حرصنا نحن على تعريفها بأنفسنا.

هناك صعوبة كبيرة في الربط بين تحرّك غُفُل الهويّة على الإنترنت، وبين شـخص محـّدد بعينـه. إذ ربما لا يكون الشـخص راغباً في التعـرّف إليه. يكتـب تعليقاً مغفل

الهويّة على أحد المواقع الشبكيّة، أو ربما يطلق هجوماً إلكترونيّاً في الفضاء السبراني بواسطة شبكتك. في تلك الحال يجب على النُظُم الرقميّة أن تجيب عن سؤال أشد صعوبة هو: «من يكون ذلك المجهول»؟

على المستوى الأساسي تماماً، لا نستطيع التعرّف إلى النُثَر المستقلّة من المُكوّنات الإلكترونيّة أو البرامج الرقميّة، عندما يتّخذ الخصم المراوغ قراراً بالتهرّب من عمليات التعرّف إلى هويّته. لا نستطيع استخلاص معلومات من حزم متناثرة من البيانات تدور في فضاء الإنترنت. لا نستطيع التثبّت من هويّة شخص مجهول يجلس خلف لوحة مفاتيح إلكترونيّة في مكان ما على الكرة الأرضيّة. وليس من المستطاع التوصّل إلى حلّ لتلك المشكلة بواسطة هندسة معيّنة للنُظُم الإلكترونيّة؛ لأنّ ذلك الضعف كامن في صلب طريقة عمل الإنترنت.

ويعني ذلك أننا لا نستطيع الجزم بشأن من ترك تعليقاً مغفل الهويّة على مُدوّنَة إلكترونيّة. (إذ يحتمل أن يكتب من كومبيوتر عام، أو حاسوب يحتوي عنواناً تعريفيّاً مشتركاً). لا نستطيع الجزم بشأن هويّة من بعث برسالة إلكترونيّة. من المستطاع تزييف المقدّمات التعريفيّة، وهو أمر يفعله من يطلقون سيول الرسائل المتطفّلة التي تشتهر باسم «سبام» (Spam). لا نستطيع الجزم بشأن آلاف المحاولات المتتاليّة الفاشلة للدخول إلى حسابك البنكي، ولا من يشن هجمات إلكترونيّة تستهدف البنية التحتيّة للبلاد.

حتى إننا لا نستطيع الجزم إن كانت تلك الهجمة الإلكترونيّة تمثّل نشاطاً إجراميّاً، أو عملاً عسكريّاً، أو التعرّف إلى الحكومة التي تقف وراءها[41]. إنّ الهجمات السبرانيّة ضد أستونيا في العام 2007، وهي غالباً ما توصف بـ «الحرب السبرانيّة الأولى»؛ إما شنّتها الحكومة الروسيّة أو شاب في الـ22 من العمر غلبته أهواؤه[42].

عندما ننجح في الربط بين هويّة ما وهجمة إلكترونيّة معينة- كالقول إنها تأتي من مدير ثانويّة سيئ الطوية، أو سارق بنك، أو مجموعة تدعمها حكومة ما- فإننا نفعل

ذلك بعد تحقيق جنائي موسّع، أو لأن المُهاجم أتاح التعرّف إليه بطريقة أو أخرى. إذ استغرق الأمر شهوراً كي يتعرّف المحلّلون إلى الصين بوصفها مصدراً محدّداً للهجمات الإلكترونيّة التي استهدفت صحيفة **نيويورك تايمس** في 2012[43]؛ كما لم نعرف تحديداً من صنع الفيروس الإلكتروني «ستاكس نت» إلى أن أقرّت الولايات المتّحدة بذلك[44]. إنها مسألة صعبة تماماً، ومن المرجح ألا نتمكن من إيجاد حلّ لها في مستقبل قريب.

على مرّ السنين، قدّمت حلولاً عدّة لوضع حد لإغفال الهويّة على الإنترنت[45]. وكانت الفكرة وراء ذلك أنّه إذا كان ممكناً ربط الهويّة بالأعمال كافة على الإنترنت- بمعنى الربط بين العمل ومصدره- يغدو من السهولة بمكان التعرّف إلى المجرمين ومطلقي بريد الـ «سبام»، والمتربصين بالناس، ومتصيّدي الثروات على الإنترنت. واختصاراً، يصبح لكل منا على الإنترنت ما يعادل رخصة القيادة.

إنّه هدف مستحيل. أولاً، لا يوجد في العالم الفعلي بنية تحتيّة لتعطي كل مستخدمي الإنترنت أوراقاً ثبوتيّة تستند إلى نُظُم التعريف الفعليّة الأخرى- جواز السفر، وبطاقة الهويّة، ورخصة القيادة وأي شيء مماثل- وهو ما نحتاجه للوصول إلى تلك النقطة من التعرّف إلى هويّات مستخدمي الإنترنت. وبالتأكيد لا نملك بنية تحتيّة من ذلك النوع تستطيع أن تشمل العالم بأسره.

حتى لو توصّلنا إلى شيء كذلك، فلسوف يستحيل جعله مأموناً. إذا عاش كل منا التجربة المقلقة لرؤية مراهقين يحاولون شراء شراب كحولي قبل بلوغهم سن الرشد، على الرغم من أن ذلك يتعلّق بمقابلة مباشرة تجري وجهاً لوجه. ولن يكون النظام المقترح أعلاه بأفضل حالاً من ذلك. وحتى لو توصّل إلى مستوىً أفضل، فلن يكون عمليّاً. ومن المستطاع دوماً وضع نظام لتغفيل الهويّة ضمن نظم التعريف بالهويّة. ويقلق بلد كالصين من تلك الحقيقة؛ لأنه يريد معرفة الهوية الحقيقيّة لكل من يستعمل الإنترنت في أراضيه[46].

لربما بدت تلك الكلمات متناقضة مع ما ورد في الفصل 3 حول سهولة التعرّف في الإنترنت إلى الأشخاص الذين يسعون لإخفاء هويّتهم. إذ يحصل ذلك بسهولة عندما تتوافر كميّات كافية من المعلومات كي تربط ببعضها بعضاً، إضافة إلى زمن كافٍ للتدقيق فيها. وتشكّل الرقابة الواسعة للجموع الطريقة الوحيدة لتقليص عمليات إغفال الهويّة على الإنترنت. وفي الفصل 3، استندت الأمثلة كلها إلى الربط بين نتف كثيرة من المؤشّرات، مع الحصول على وقت كافٍ للتحقيق فيها. في المقابل، يغدو صعباً بما لا يقاس التدقيق في كل اتّصال إلكتروني على الإنترنت وصولاً إلى مصدره، كأن يجري التدقيق في كل رسالة إلكترونيّة وحيدة، ووصلة شبكيّة مفردة وهجمة رقميّة بمفردها.

يبقى السؤال مفتوحاً عن مدى القدرة على إيكال عمليات التعرّف إلى الهويّة بتحليل البيانات وربطها إلى الآلات الذكيّة. هل من المستطاع صنع نظام حاسوبي متقدّم الذكاء بما يتيح له تحليل معلومات الرقابة للتوصّل إلى التعرّف إلى الهويّات الفرديّة للناس بما يشبه الأمثلة التي عرضها الفصل 3، على نطاق واسع تماماً؟ ربما لا نملك ذلك الآن، ولكن الوقت لن يطول قبل ظهور نظام كذلك.

ثمة جهود تبذل في ذلك الاتّجاه. إذ ترغب بلدان كالصين وروسيا في صنع نُظُم مؤتمتة للتعرّف إلى هويّة الأصوات المُعارِضَة على الإنترنت. وتسعى شركات الترفيه للحصول على نُظُم مُشابِهَة للتعرّف إلى من يقرصنون الأفلام والموسيقى. وترغب حكومة الولايات المتّحدة بتلك النُظُم كي تتعرّف إلى المنظّمات والأشخاص الذين تحسّ بأنهم يمثلون خطراً عليها، بداية من الأفراد المعزولين ووصولاً إلى الحكومات الأجنبيّة.

في 2012، صرح وزير الدفاع ليون بانيتا علانية بأن «الولايات المتّحدة أحرزت تقدّماً ملفتاً... في التعرّف إلى مصادر الهجمات السبرانيّة[47]». ويذهب بي الظن إلى أن أميركا لم تحرز تقدّماً جديداً في هندسة الكومبيوتر وعلومه يكفل لها قلب الموازين

جذريّاً في التوازن بين عمليات التعرّف إلى الهويّة وإغفالها على الإنترنت. والأرجح أنها نجحت في اختراق شبكات الخصوم بشكل عميق إلى حدّ يكفل لها التجسّس عليهم والتعرّف إلى خططهم.

بديهي القول أيضاً إن تغفيل الهويّة سيف ذو حدّين؛ لأنه ربما استُخدِم لحماية خطابات الكراهية والنشاط الإجرامي. ولكن، بينما يصح الحديث عن أهمية عمليات التعرّف إلى الهويّة، فإن تغفيل الهويّة مهم أيضاً للأسباب التي بيّنتها في هذا الفصل. ويعني ذلك أنها تحمي الخصوصيّة، وتزيد في تمكين الأفراد، إضافة لكونها شرطاً أساسيّاً للحريّة.

11

الأمن

يمتلك الأمن أهمية كبيرة في حياتنا. وتشكّل الجريمة والإرهاب والعدوان الخارجي تهديدات تطالنا في الفضاء الافتراضي وخارجه. بديهي القول إنها ليست التهديدات الوحيدة، لكنني صرفت معظم الفصول السابقة في تبيان تهديدات أخرى. تلزمنا حماية من مجموعة تهديدات متكاملة، ومن هذه النقطة تبدأ المشكلات. لا جدوى من إنكار خطر الأجهزة الشرطية المتغوّلة أو الحكومة الطاغية، بدعوى حماية أنفسنا من الإرهاب؛ أو إنكار خطر الإرهاب بهدف النجاة من انفلات الأجهزة الشرطية.

وللأسف، عندما يميل المجتمع إلى التركيز على خطر معيّن، فإنّه غالباً ما يهوّن من شأن بقية المخاطر. والأسوأ من ذلك أننا نميل إلى التركيز على خطر نادر عندما يسدد ضربة مشهدية ضخمة، فيما نتجاهل مخاطر أكثر شيوعاً وتكراراً وعاديّة[1]. ولذا، نخاف من الطيران أكثر من قيادة السيارة، على الرغم من أن الأولى أكثر أماناً. ونخشى الإرهابيّين أكثر من الشرطة، على الرغم من أن الأميركي معرّض لأن يقتل على يد ضابط شرطة بتسعة أضعاف تعرضه للموت على يد إرهابي[2].

بذا، تعترض المخاوف طريق التوصّل إلى أمن ذكي. ليس من بُعد النظر الاتّكال على استراتيجية تحمي من مخاطر معيّنة على حساب أخرى، بل يجدر بنا التوصّل إلى طُرُق تضمن التوازن في ضمان الأمن ضد المخاطر كلها.

الأمن في مواجهة الإرهابيّين والمجرمين

استخدمت «وكالة الأمن القومي» تكراراً صورة مجازيّة هي «التوصيل بين النقط»؛ كي تبرّر نشاطاتها الرقابيّة[3]. ومرّة تلو الأخرى؛ بعد ضربات 9/ 11، وعقب المفجّر الذي دسّ متفجرات في ملابسه الداخلية، وبعد تفجيرات «ماراثون بوسطن» وغيرها؛ انتُقِدَت الحكومة لأنها لم تعمل على التوصيل بين النقط.

في المقابل، إنّ تلك الصورة المجازية عن توصيل النقط لهي مضلّلة تماماً. إذ يسهل التوصيل بين النقط في كتب الرسم الملوّنة المعدة للأطفال؛ لأنها مرقمة ومرئيّة بوضوح. أما في الحياة الفعليّة، فلا ترى النقاط إلا بعد ظهور حقائق.

لا يمنعنا ذلك من الإلحاح على معرفة سبب عدم قيام الحكومة بتوصيل النقط[4]. وبرؤية استرجاعيّة، يمكن القول إن هنالك علامات منذرة صدرت بوضوح عن مفجّر مطلق النار في ثكنة «فورت هود»، مفجّرَي «ماراثون بوسطن»، ومطلق النار في مدرسة «إيسلا فيستا». يسمّي الكاتب نسيم طالب ذلك الأمر بـ «مغالطة السرد»[5]. ومن طبيعة البشر الميل إلى إخبار القصص، وغالباً ما يكون عالم القصّة أكثر انتظاماً وتوقّعيّة وانسجاماً من العالم الفعلي. إذ يتصرّف ملايين الناس بطرق فيها من الغرابة ما يكفي للفت أنظار الـ «إف بي آي»، لكن غالبيتهم الساحقة لا يشكّلون خطراً. تضم قائمة «أمن إدارة النقل» قرابة عشرين ألف شخص ممنوعين من السفر جوّاً[6]. وتحتوي القائمة المعروفة باسم «قائمة الموضوعين تحت الرقابة»[7]، قرابة 680 ألف شخص، لكن 40 ٪ منهم «لا يملكون انتماءات معروفة لتنظيمات إرهابيّة».

يُقدّم التنقيب في المعلومات بوصفه التقنيّة الكفيلة بتمكيننا من توصيل النقط. وتنجح الشركات تماماً في التنقيب في بياناتنا الشخصيّة كي توجّه إعلاناتها بدقّة، وترصد التزوير المالي وتنهض بمهام أخرى، فيما تنتصب ثلاث قضايا حسّاسة في وجه تحوّل التنقيب في البيانات أداة كفؤة في العثور على الإرهابيّين.

تتجسّد القضيّة الأولى والأكثر أهميّة في معدلات الأخطاء. ففي الإعلانات، يكون التنقيب في المعلومات أداة ناجعة حتى في ظل نسب مرتفعة من معدلات الأخطاء، لكن العثور على الإرهابيّين يتطلّب درجة من الدقّة أعلى كثيراً، ليس بوسع نُظُم التنقيب في البيانات تحقيقها.

إذ يكون التنقيب في المعلومات ناجحاً عندما تبحث عن بروفايل محدّد تماماً، وعندما تكون هناك مناسبات متكرّرة سنويّاً ويكون ثمن الإنذار الخاطئ زهيداً. ويقدّم تقصي تزوير بطاقات الائتمان قصة نجاح بارزة لقدرة التنقيب في البيانات في مجال الأمن[8]. وتنقّب شركات البطاقات الائتمانيّة كلها في قواعد بياناتها للعثور على نمط من الإنفاق يوحي بسرقة بطاقة ائتمان. في الولايات المتّحدة، يجري التداول بقرابة بليون بطاقة ائتمان مفعّلة، ويطاول التزوير قرابة 8 ٪ منها[9].

يتشارك كثير من بطاقات الائتمان المسروقة في نمط معيّن- هو الشراء من أمكنة غير مألوفة بالنسبة لصاحب البطاقة الأصلي، إضافة إلى شراء سلع سياحيّة مترفة، وأشياء يسهل حملها- ما يعطي نُظُم التنقيب في المعلومات القدرة على تقليص الخسائر بكشفها معاملات ماليّة مزوّرة. ولا تزيد كلفة الإنذار الخطأ عن مكالمة تليفونيّة لصاحب البطاقة تطلب منه تأكيد حصول بعض عمليات الشراء.

وعلى نحوٍ مماثل، تستخدم «وكالة المداخيل الداخليّة» تقنية التنقيب في البيانات للتعرف إلى المتهرّبين من الضرائب[10]؛ كما تستعملها الشرطة لتعيين النقاط الساخنة المرشحة لحدوث جرائم فيها[11]؛ كما تستخدمها البنوك لتوقّع حالات عدم القدرة على سداد الديون. نالت تلك الأنماط من استخدام تقنية التنقيب في المعلومات حظوظاً متفاوتة من النجاح، وفقاً لنوعيّة المعلومات والبرامج، لكنها تظل ضمن إطار ما تستطيع تلك التقنية إنجازه.

يختلف الأمر مع مخطّطات الإرهابيّين، غالباً بسبب كثرة المعاملات المزوّرة مقابل ندرة ضربات الإرهاب[12]. ويعني ذلك أن نُظُم توقّع الإرهاب تبقى مكتظّة بالإنذارات المغلوطة، مهما كانت دقّة النُظُم عالية[13].

يعود السبب في ذلك إلى رياضيات نُظُم التنقيب في البيانات. هناك أخطاء في نُظُم التقصي كلّها، ويستطيع مصمّمو النُظُم ضبطها بما يكفل تقليل هوامش الإنذارات الكاذبة إيجابيّاً أو المغلوطة سلبياً. وفي نُظُم تقصي الإرهابيّين، يكون الإنذار كاذباً إيجابيّاً عندما تُنْذِر خطأً عن شيء بريء بوصفه خطيراً. ويحدث الإنذار الكاذب السلبي عندما تفشل النُظُم في توقّع حدوث ضربة إرهاب. ومن المستطاع ضبط النُظُم بما يزيد إمكان صدور إنذارات كاذبة إيجابيّاً (وحينها تضبط النُظُم كي لا تترك أي شيء من دون الاشتباه فيه)، أو لزيادة تلك النسبة، بمعنى ضبط النُظُم كي تعطي عدداً أقل من الإنذارات الكاذبة إيجابيّاً لكن على حساب زيادة احتمال الفشل في تقصي هجمات إرهابيّة.

ولأن الضربات الإرهابيّة نادرة عدديّاً، تؤدّي زيادة عدد الإنذارات الكاذبة إيجابيّاً إلى إرهاق نظام ملاحقة الإرهابيّين برمّته، مهما كانت الدقّة في ضبط النُظُم[14]. وأنا استعمِل كلمة «برمّته» عامداً، للإشارة إلى أن ملايين الأشخاص سوف يتّهمون خطأً عند اكتشاف أي مخطط إرهابي، بافتراض أن النُظُم تمكّنَت من ذلك[15].

ربما نستطيع التعامل مع حال يوضع فيها ملايين الناس في خانة الاشتباه، لو كانت تكلفة الإنذار الكاذب إيجابيّاً متدنيّة. فكّر بالماسحات الضوئيّة التي تمر فيها أجساد الناس في المطارات. إنّها تصدر دوماً إنذارات إيجابيّة كاذبة، لكن الأمر لا يتطلب سوى أن يربت المفتش على المسافر كي يعرف الخطأ. لا يسير الأمر على ذلك النحو بالنسبة لنُظُم تقصي الإرهاب التي يشمل عملها الناس عموماً. إذ يتطلّب كل إنذار إيجابي كاذب إنجاز تحقيقات مطوّلة لتحديد مصداقيته. يقتضي ذلك إنفاق

كثير من الجهد والوقت، ويعيق المحقّقين عن إنجاز أعمال أكثر جدوى. وبقول آخر أشد وقعاً، إذا كنت تراقب كل شيء فلن ترى شيئاً.

كذلك يتداول مجتمع الاستخبارات الأميركيّة تشبيهاً عن مخطّطات الإرهاب هو البحث عن إبرة في كومة قش. ووفق كلمات المدير السابق لـ «وكالة الأمن القومي» كيث آلكسندر، «أنت تحتاج إلى كومة قش كي تبحث فيها عن إبرة». تعبّر تلك الجملة بالضبط عن مشكلة الرقابة العامة والتجميع الضخم للمعلومات. عندما تبحث عن إبرة في كومة قش، فإنّ آخر ما تتمناه هو إضافة مزيد من القش على الكومة[16]. بقول أكثر تحديداً، ليس من مبرّر علمياً للاعتقاد بأن صبّ مزيد من البيانات العشوائيّة عن الناس، يزيد في سهولة اكتشاف مخطّطات الإرهاب، وهناك شواهد كثيرة على ذلك. إذ ربما ضمّت تلك المعلومات إشارة ذات دلالة، لكن مقابل ذلك فإنّها تضيف كثيراً من التشوّش[17]. وعلى الرغم من عقليّة «لنجمع كل شيء» السائدة في «وكالة الأمن القومي»، فإن وثائقها بالذات تدحض جدوى ذلك التفكير. أكثر من ذلك، يتحدث مجتمع الاستخبارات العسكريّة عن «الشرب من أنبوب النار»، بمعنى الحصول على كميّات ضخمة من المعلومات المفتقدة إلى الدلالة، مع ضياع تلك التي تحمل دلالة فعليّاً[18].

تبدّت تلك النقطة في برنامج «وكالة الأمن القومي» للتنصّت الإلكتروني، إذ فاقت الإنذارات الكاذبة إيجابيّاً القدرة على التعامل معها. في سنوات ما بعد 9/ 11، قدّمت «وكالة الأمن القومي» آلاف التلميحات إلى الـ «إف بي آي» شهريّاً، لكنها كانت إنذارات إيجابيّة كاذبة[19]. كانت تكلفة ذلك الحال ضخمة، وانتهى الأمر إلى إحباط ضبّاط الـ «إف بي آي» الذين أجبِروا على تقصي كل دليل محتمل. ظهر الأمر عينه في قاعدة البيانات المسمّاة «تقارير النشاطات المشتبه فيها» (Suspicious Activities Reports) التي جمعت عشرات آلاف التقارير لكنها لم تعطِ نتائج فعليّاً[20]. ولم تؤدّ كل الـ «ميتاداتا» التي جمعتها «وكالة الأمن القومي» إلا إلى نجاح يتيم[21]: اعتقال سائق سيّارة أرسل 8500 دولار إلى تنظيم في الصومال لا يمثّل

تهديداً مباشراً لأمن الولايات المتّحدة. وجرى التطبيل والتزمير لذلك الإنجاز، ربما لإعطاء «وكالة الأمن القومي» فرصة تسجيل نقاط في حوارها مع الكونغرس[22].

تمثّل الفرادة التي تتمتّع بها مخطّطات الإرهاب القضية الثانية التي تعيق استعمال تقنية التنقيب في المعلومات لمحاولة الكشف عن مخطّطات إرهابيّة[23]. من كان يدري أنّ طنجرتَيْ ضغط تصبحان قنبلتين محمولتين في حقيبتي ظهر لطالبين جامعيّين في بوسطن، هما شاب وأخوه الكبير؟ كلما نفّذ شخص يندر توقع انخراطه في الإرهاب هجمة ما؛ فإنّه يولّد أثراً أضخم مما نفّذه عمليّاً بالنسبة للمعايير المعتمدة في توقّع الأشخاص الذين يحتمل أن يكونوا إرهابيّين، فتختل استراتيجيّات ترصد الإرهابيّين.

تظهر القضية الثالثة المعيقة للاستفادة من تقنية التنقيب في البيانات للكشف عن مخطّطات إرهاب، في أن الأشخاص الذين تلاحقهم «وكالة الأمن القومي» يتّسمون بالمراوغة، ويسعون إلى التملّص من تتبع نشاطاتهم على الإنترنت. في عوالم التسويق المشخصَن، لا يسعى الشخص عادة إلى إخفاء نشاطاته على الإنترنت. ولا ينطبق ذلك الوصف في سياق عمل الشرطة والأمن القومي. تؤدّي تلك العلاقة التصارعيّة [بين الأجهزة الأمنيّة والإرهابيّين المحتملين على الإنترنت] إلى جعل الأمور *أشد* صعوبة، ما يعني أن معظم أدوات تحليل «البيانات الضخمة» المتوفرة في السوق لا تستطيع التعامل مع أحوال الإرهاب. إذ يمكن لأدوات السوق أن تتجاهل ببساطة الأشخاص الذين يتهرّبون منها، إضافة إلى أنها تفترض سلوكاً حميداً من قِبَل بقية الأفراد كافة. ولا تستطيع الأدوات التي تستخدمها الحكومة في تحليل البيانات تبنّي تلك المقاربة؛ لأنها تسعى بالضبط إلى التقاط الأشخاص المراوغين.

يتفاوت أولئك الأعداء في مدى تقدّم قدرتهم على تجنّب الرقابة. ولا يمتلك معظم المجرمين والإرهابيّين- وكذلك الحال بالنسبة للمنشقين سياسيّاً، وهو

أمر من المؤسف قوله- تمرّساً كافياً في التملص من الرقابة الإلكترونيّة، ولذا فهم يرتكبون أخطاء جمّة. ولا يصلح ذلك تبريراً للجوء إلى تقنية التنقيب في المعلومات، خصوصاً أن الرقابة الموجّهة تستطيع الوصول إليهم. يجدر السؤال عن الفارق بين الرقابتين العامة والموجّهة في الوصول إلى أولئك الأشخاص، وإذا كان الفارق يبرّر الأكلاف العالية المتّصلة بالرقابة العامة. وأظهرت مجموعة من التحليلات لجهود «وكالة الأمن القومي» أن الأمر ليس كذلك أبداً[24].

إذاً، لا يمكن إصلاح القضايا الثلاث التي أثيرت آنفاً. ببساطة، يشكّل التنقيب في البيانات أداة من الخطأ استعمالها لتقصي الإرهابيّين، ما يعني أنه لا يمكن تبرير فرض رقابة عامة[25]. وعندما كان مديراً لـ «وكالة الأمن القومي»، حاجج كيث آلكسندر بأن الرقابة الشاملة كانت كفيلة بتمكين الوكالة من اكتشاف مخططات 9/ 11[26]. لا يبدو ذلك أمراً مرجّحاً. إذ لم يتمكن آلكسندر من درء تفجيرات «ماراثون بوسطن» في 2013، على الرغم من أن أحد المُفجّرين كان موجوداً على لائحة المراقبة الخاصة بالإرهابيّين، وترك المُفجّران آثاراً كبيرة تتصل بمخطّطهما في وسائط التواصل الاجتماعي[27]. وحدثت تلك التفجيرات بعد ما يزيد على عشر سنوات من 9/ 11، حدثت فيها قفزات كبرى في التقنيّات المتصلة بالرقابة. وكانت لدى «وكالة الأمن القومي» معلومات جمّة عن الإخوة تسارناييف قبل تنفيذهما تفجيرات «ماراثون بوسطن»، لكن الوكالة لم تلاحظ فارقاً بين تلك المعلومات وما جمعته عن ملايين الناس[28].

أثيرت تلك النقطة ضمن تقرير لجنة التحقيق في 9/ 11 الذي تحدّث عن الفشل «في توصيل النقط»، الذي يرى فيه مؤيّدو الرقابة العامة مبرّراً لجمع كميّات من المعلومات تتزايد باطّراد. ولاحظ التقرير أن مجتمع الاستخبارات الأميركي استطاع تجميع معلومات عن ذلك المخطط، من دون اللجوء إلى الرقابة العامة، منبّهاً إلى أن الفشل تأتّى فعليّاً من التحليل غير المناسب للمعلومات[29].

لم تستطع الرقابة الشاملة الإمساك بالملابس الداخليّة للمُفجّر عمر فاروق عبد المطّلب في 2006، على الرغم من أنّ أباه حذّر الحكومة الأميركيّة تكراراً من كون ابنه خطيراً[30]. وفي العام 2006، عُثِر على المتفجّرات السائلة[31] - وهي الحجّة التي تستخدمها الحكومات في منع المسافرين جوّاً من وضع زجاجات كبيرة من السوائل والكريمات والـ «جيل» في حقائب اليد التي يحملونها معهم إلى الطائرة- في شقّة في لندن جرى تحديدها بفضل تحقيق بوليسي بوسائل تقليديّة، وليس بواسطة رقابة عامة. وفي الحالات المعروفة عن نجاح «وكالة الأمن القومي»، كانت المعلومات تأتي دوماً من الرقابة الموجّهة، وليس برقابة عامة[32]. وبيّن أحد التحليلات أنّ الـ «إف بي آي» تتعرّف إلى مخطّطات إرهابيّة محتملة بواسطة تقارير عن النشاطات المشبوهة[33]، وتقارير عن مخطّطات لارتكاب جرائم أخرى، وكذلك من التحقيقات المتعلّقة بتلك الجرائم.

إنّها نقطة حاسمة. إذ لا تمثّل الرقابة الشاملة ولا تقنية التنقيب في المعلومات أدوات مناسبة للعثور على إرهابيّين ومجرمين. وتُبدّد بلايين من دولارات دافعي الضرائب على برامج الرقابة العامة، من دون الحصول على الأمن الذي تعدنا به. وهناك ما هو أشد أهمية من ذلك، بمعنى أن الأموال تبدّد على تلك البرامج اللامجدية للرقابة العامة، بدل إنفاقها على التحقيق والاستخبارات والاستجابة للحالات الطارئة؛ وكلها تكتيكات أثبتت جدواها[34].

تصلح الرقابة العامة وتقنية التنقيب في البيانات في مهمات تتعلّق بالتمييز بين عموم الناس، بمعنى العثور على أصحاب ميول سياسيّة معيّنة، وأولئك الذين يصادقون شخصيّات بعينها، والأعضاء في جمعيات سريّة، والأفراد الذين يرتادون لقاءات وتظاهرات محدّدة. يكون أولئك الناس موضع اهتمام حكومات تميل للسيطرة على المجتمع، كالصين. ويرجع سبب نجاعة استخدام تقنية التنقيب في المعلومات في كون المنشقّين سياسيّاً، على غرار مزوّري بطاقات الائتمان؛ يتشاركون بصورة عامة في بروفايلات محدّدة. ويضاف إلى ذلك أنّ الحكم المتسلّط لا يكترث

لمسألة الإنذارات السلبيّة الكاذبة؛ لأن إدانة البريء بتهمة التحريض على العصيان ينشر الخوف في قلوب العامة.

وإضافة إلى كونها غير فعّالة، فإن الرقابة العامة التي تمارسها «وكالة الأمن القومي» تجعلنا عمليّاً أقل أمناً. ولتبيان جليّة ذلك الأمر، يجب علي أن أتوسّع قليلاً في شرح أمن الإنترنت ومسألة التشفير ونقاط الضعف في نُظُم الكومبيوتر. وتبيّن المقاطع الثلاثة التالية تلك الأمور، ما يجعلها مقاطع مهمّة أيضاً.

الهجوم مقابل الدفاع في الإنترنت

في الأوضاع الأمنيّة كافة، يحدث سباق في التسلّح بين الهجوم والدفاع. يكسب أحد الطرفين السباق لفترة ما، ثم تتبدّل التقنيّة ويكسب الطرف الآخر تفوّقاً، ثم تتغيّر الأحوال كرّة أخرى.

فَكِّر في تاريخ التقنيّات العسكريّة وتكتيكاتها. في مطالع القرن التاسع عشر، مالت الكفّة لمصلحة الميّالين إلى الأساليب الدفاعيّة؛ ذلك أن تحطيم خط دفاعي كان أكثر كلفة من حمايته. كان نابليون بونابرت سبّاقاً في التفكير في أساليب الهجوم الفعّالة مع استخدام الأسلحة التي كانت متوفّرة في ذلك الوقت. ومع الحرب العالمية الأولى، حازت الأسلحة الناريّة- خصوصاً الرشاشات الثقيلة- حدّاً كبيراً من القوّة، فمالت الكفّة مجدّداً صوب الأساليب الدفاعيّة؛ لأن أسلحة المتحصنين كانت قمينة بحصد المهاجمين. وانقلبت موجة المدّ ثانية في الاتجاه المعاكس مع الحرب العالمية الثانية، مع التسليح المتطوّر للدبابات والمدرّعات الميكانيكيّة، ما أعاد الأفضليّة إلى أساليب الهجوم.

وحاضراً، يمتلك المهاجم الأفضليّة على شبكة الإنترنت ونُظُم الكومبيوتر عموماً[35]. وهناك أسباب تفسّر ذلك:

* يسهل تحطيم الأشياء ولكن يصعب إصلاحها[36].

* يعدُّ التعقيد العدو الأسوأ للأمن، وتسير نُظُم المعلوماتيّة باطّراد نحو مزيد من التعقيد[37].

* تسهّل طبيعة نُظُم الكومبيوتر للمهاجم العثور على نقطة ضعف قابلة للاستغلال، فيما يجب على المدافع معرفة نقاط الضعف *كلها* ثم العمل على إصلاحها.

* يستطيع المُهاجِم أن يختار هجمة ما ويركّز جهوده عليها، فيما يفترض بالمُدافع أن يتحسّب لأنواع الهجمات كلها.

* غالبيّة البرامج الرقميّة ضعيفة أمنياً[38]. وببساطة، ليس من السهل كتابة برامج آمِنة، وإنشاء نُظُم كومبيوتر آمنة. نعم، هناك تطوّر يحدث باستمرار في ذلك الصدد، لكن الأمر لم يصل بعد إلى المستوى المطلوب.

* الأمن المعلوماتي هو شأن تقني معقّد، ومن السهل أن يقع المستعمل العادي في الخطأ، فيخرّب ما صُنع لحمايته.

ليس من السهل القول إنّه لا جدوى من أمن الإنترنت، لأن الأمر بعيد عن ذلك. فعلى الرغم من سهولة الهجوم، فإن الدفاع ما زال ممكناً. إذ تتكفّل الحماية الجيّدة بجعل الهجمات أشد صعوبة، وأعلى كلفة وأشد خطورة على منفّذيها. وإذا لم يكن المُهاجِم متمرّساً، يستطيع الأمن المعلوماتي توفير حماية كاملة منه.

في حقل الأمن، يتمحور التفكير حول إدارة المخاطر. ويجب أن تعرف ما الخطر الذي تواجهه، وما هو الأسلوب العقلاني في التحوّط منه. وبالنسبة لكل من لديه كومبيوتر في المنزل، يجب الحصول على برنامج جيّد في الأمن المعلوماتي، والحرص على الاستفادة دوماً من التجديدات، وتجنّب المواقع الشبكيّة المشبوهة، وتفادي قراءة مرفقات الرسائل الإلكترونيّة الآتية من أشخاص مجهولين، والحرص على الاحتفاظ بنسخ احتياطيّة. تستطيع تلك الخطوات وغيرها من الإجراءات الأمنيّة الأساسيّة

أن تجعلك منيعاً حيال مجرمي الإنترنت العاديّين والـ «هاكرز» غير المتمرّسين. من ناحية أخرى، إذا كنت منشقاً سياسيّاً في الصين أو سوريا أو أوكرانيا، وتحاول تجنّب الاعتقال أو الاغتيال؛ يجدر بك اللجوء إلى إجراءات حماية أكثر شمولاً واتّساعاً. وتنطبق النصائح السابقة عينها إذا كنت مجرماً تحاول التهرّب من الشرطة، أو رجل أعمال يحاول منع تجسّس الشركات الأخرى على أعماله، أو سفارة رسميّة تسعى إلى صد التجسّس العسكري عليها. وإذا كان لديك قلق خاص تجاه المعلومات التي تجمعها الشركات عنك، فلسوف تحتاج إلى مجموعة أخرى من إجراءات الأمن المعلوماتي.

بالنسبة لعدد من الشركات، تُردّ مسألة الأمن إلى الحسابات الأساسيّة اقتصاديّاً. إذا كانت تكلفة الأمن أقل من الخسائر الناجمة عن غيابها، تميل الكفة إلى الأمن. إذا فاقت تكلفة الأمن ما تحدثه الهجمات من خسائر، يكون الحل في تقبّل الخسائر. بالنسبة للأفراد، هناك كثير من المزج بين البعد النفسي والاقتصادي. إذ يصعب احتساب الكلفة الماليّة الناجمة عن فقدان الخصوصيّة، أو من وضع أسماء الأفراد على لوائح المراقبة. وعلى الرغم من ذلك، تبقى المعادلة على حالها: الكلفة مقابل الاستفادة.

من الأهمية بمكان في هذا التحليل ملاحظة الفارق بين الهجمات العشوائيّة والموجّهة.

تتسم غالبيّة الهجمات الإجراميّة بالانتهازيّة. في العام 2013، دخلت مجموعة من الـ «هاكرز» إلى الشبكة الداخلية لسلسلة محلات «تارغت» للبيع بالتجزئة، وسرقوا معلومات عن 40 مليون شخص تتعلق ببطاقات الائتمان وبيانات شخصيّة متنوّعة[39]. وحينها، وُصِفَ ذلك الاختراق بأنّه الأضخم، وتسبّب بكارثة للشركة[40] استقال إثرها مديرها التنفيذي، كريغ شتاينهافل[41]؛ لكن المجرمين لم يختاروا استهداف «تارغت» تحديداً لأي سبب أيديولوجي. إذ انصب اهتمامهم

على أرقام بطاقات الائتمان كي يتمكنوا من تزويرها؛ وكانوا ليفعلون الأمر نفسه مع أي شركة أخرى. لو امتلكت «تارغت» نظاماً أشد متانة في الأمن المعلوماتي، لتوجّه المجرمون إلى شبكات أخرى. يشبه أمرهم أمر السارق التقليدي للبيوت. إذ هو يسعى إلى سرقة بيت، ولربما كانت لديه خيارات بالنسبة لنوعية البيوت والأحياء، لكنه لا يكترث للبيت الذي يتمكن من سرقته. وتتمثّل مهمّتك كمالكٍ للبيت في جعل منزلك أقل إغراءً للسارقين من المنازل المجاورة لك. وللتصدي لهجمات غير موجّهة، يكون الأمن الجيد مسألة نسبيّة.

قارِن ذلك مع هجمات العام 2012 على صحيفة نيويورك تايمس من قِبَل «هاكرز» صينيّين ربما كانوا على صلة بحكومة بلادهم[42]. في تلك الحال، سعى المهاجمون إلى ترصد اتّصالات مراسلي الصحيفة مع منشقّين صينيّين. واستهدفوا تحديداً البريد الإلكتروني لنيويورك تايمس وشبكتها الرقميّة الداخليّة؛ لأنها الأمكنة التي تحتوي على المعلومات التي يسعون إليها. في حال الهجمات الموجّهة، ما يصنع الفارق هو المستوى المطلق للأمن. لا يتعلّق الأمر بأن سرقة جارك ربما تكون أسهل؛ لأن المهاجم يستهدفك تحديداً، ما يعني وجوب أن تمتلك قدرات دفاعيّة تستطيع التصدي لإمكانات من يهاجمونك تحديداً.

هناك مثل آخر على ذلك الأمر. يعرف عن شركة «غوغل» أنها تمسح بانتظام بريد «جي ميل» الإلكتروني، وتستخدم المعلومات التي تحصدها في توجيه الإعلانات إلى الجمهور. بالطبع، لا يجري ذلك على يد موظّف بعينه في «غوغل»، بل تنهض الحواسيب بتلك المهمة. لذا، فإذا كتبت بريدك الإلكتروني بلغة غير مألوفة لا يستطيع «غوغل» ترجمتها أوتوماتيكيّاً، سوف تكون في مأمن من المسوحات التي يجريها «غوغل» باستخدام جداوله الخوارزميّة الخاصة؛ فليس مجدياً لتلك الشركة أن تترجم يدويّاً رسائلك الإلكترونيّة. لكن، إذا صرت فجأة هدفاً لتحقيق موجّه يجريه الـ «إف بي آي»، سوف يخصّص المحققون وقتاً للترجمة اليدويّة للرسائل الغامضة في بريدك الإلكتروني.

تذكّـر دوماً هذا الفارق الأمني بين الرقابة العامة والرقابة الموجّهة؛ لأننا سـنعود مراراً وتكراراً إليه.

قيمة التشفير

قدّمت الكلمات السـابقة وصفاً لأمن الإنترنت كنوع من سـباق التسـلّح يمتلك فيه المُهاجم أفضلية على المُدافع. ربما تكون الأفضلية كبيرة، لكن يبقى أن لها حدوداً. لا يكـون الأمر أبـداً أن طرفاً ما يحوز تقنية فائقة القـوّة إلى حـدّ أن الطرف الآخر لا يستطيع الانتصار عليها، على خلاف ما يظهر في الأفلام والكتب المصوّرة.

التشـفير، بل كتابة الشـيفرة عموماً، هو استثناء. لا يقتصر الأمر على كون الدفاع أشـد سـهولة مـن الهجوم، بل إنّـه أكثر سـهولة إلى حـدّ أن الهجوم يغدو مسـتحيلاً بصورة أساسيّة.

ثمـة أفضليّـة رياضيّة بنيويّة متأصّلة بين كتابة الشـيفرة، بالمقارنـة مع محاولة كسر التشفير. أساساً، يستند الأمن المعلوماتي إلى طول مفاتيح الشيفرة، وإذا حدث أضأل تغيـير في طـول المفتاح، فسـيفرض ذلك على المهاجـم عملاً إضافيّاً فائـق الضخامة. وتتضخم تلك الصعوبة بما يشبه الانتقال من رفع العدد إلى قوة 2 ثم 3 ثم 4 وهكذا دواليـك. ربـما يسـتغرق المُهاجِم يومـاً كي يكسر مفتاحـاً من 64 بايـت، لكنه يحتاج ضعفـي ذلـك الوقت إذا زاد طول المفتـاح إلى 65 بايت. وعند صنع مفتاح من 128 بايـت، يتطلّـب ذلك ضعفي الزمن في كتابة الشـيفرة، يحتاج المُهاجِـم إلى زمن أطول بمقـدار الضعفـين مرفوعـاً إلى قوة 264، ما يسـاوي مليـون بليون سـنة من العمل الإضافي لكسر تلك الشيفرة. (للمقارنة، يبلغ عمر الكرة الأرضيّة 4.5 بليون سنة).

لذا تسـمع عبارات من نوع «سـوف يسـتغرق كسر هذه الشـيفرة زمناً يسـاوي استنفاذ طاقة الحرارة من الكون بأكمله، حتى لو افترضنا أن المُهاجِم صنع كومبيوترا باستخدام الذرات الموجودة في الكرة الأرضيّة بأكملها».

يصح قول ذلك نظرياً على الأقل. المشكلة أن الشيفرة هي حزم من المعادلات الرياضيّة، لكن الرياضيّات لا وكالة لها. عند السعي إلى تحويل تلك المعادلات الرياضيّة إلى شيء يمنحك بعض الحماية، يتطلّب الأمر كتابة ذلك بواسطة شيفرة الكومبيوتر. كذلك يجب أن تُفعّل تلك الشيفرة على الكومبيوتر الذي يحتوي أجهزة ومكوّنات إلكترونيّة صلبة، ويعمل بنظام تشغيل، كما يحتوي على برامج متنوّعة. كما يفترض أن يدير شخص ما ذلك الكومبيوتر الذي يفترض توصيله بشبكة رقميّة أيضاً. وتتكفل تلك الأشياء جميعها بإدخال عناصر الهشاشة إلى الشيفرة، ما يهزّ التكامل الذي تأتّى لها من معادلات الرياضيّات. ويعود ذلك بنا إلى نقاش حال الأمن التي عرضناها من قبل، وهي منحازة بشدّة للمُهاجِم.

بالتأكيد، تملك «وكالة الأمن القومي» بعض الرياضيّات السريّة مع قدرات هائلة في الحوسبة، ما يمكنها من كسر بعض أنواع التشفير بسهولة نسبيّة. وكذلك بَنَتْ «مؤسّسة البحوث المتعدّدة البرامج» في «أوك ريدج» بولاية تينيسي، لتلك الغاية[43]. ولكن، مهما كانت قدرات التشفير وكسره متقدّمة في «وكالة الأمن القومي»، فإن وثائق سنودن تظهر أنها تستفيد بشكل واسع من نقاط ضعف وهشاشة لدى آخرين- كأن يكونوا أشخاصاً أو حواسيب أو شبكات- للالتفاف على التشفير، بدل الاصطدام به مباشرة. تخترق «وكالة الأمن القومي» النُظُم الإلكترونيّة، وهو عين ما يفعله مجرمو الإنترنت. وكذلك ألّفت مجموعة محترفة اسمها «عمليات النفاذ المرسومة»، تتولى اختراق الشبكات وسرقة مفاتيح التشفير. وكذلك تستغل الوكالة كلمات المرور السيّئة التركيب، والمفاتيح الضعيفة وتلك المعرّفة سلفاً من قِبَل النظام الإلكتروني الذي تسعى إلى اختراقه. وخلسة، تدس الوكالة شفيرات ضعيفة في المنتجات الإلكترونيّة والرقميّة، بما فيها البرامج الرقميّة والمعايير الإلكترونيّة[44].

في العام 2013، صاغ سنودن ذلك في حوار على الإنترنت على النحو التالي: «التشفير مفيد عمليّاً. وإذا نُفّذ بطريقة ملائمة، يكون باستطاعتك الاعتماد على

نظام جيّد التشفير. ولسوء الحظ، فإن الأمن عند نقاط التقاطع بين التشفير والنُظُم والأدوات يكون هشاً بصورة مريعة، ما يمكّن «وكالة الأمن القومي» من الالتفاف حوله دوماً»(45).

وفي المقابل، تبين الطرق الأخرى التي تلجأ إليها الوكالة لضرب التشفير مدى أهميته. وعندما يتمكن التشفير من التوصّل إلى تعديل الكفّة في الرياضيات، يُجبر المُهاجِم على اللجوء إلى طُرُق أخرى. وبدلاً من التنصّت بسكون على أقنية الاتّصالات وجمع المعلومات عن الجميع، ربما وجب على المُهاجِم اختراق نظام كومبيوتر معيّن وسرقة النصوص مباشرة. تفرض تلك الطُرُق في الالتفاف حول التشفير بذل جهد أكبر، والتعرّض لمخاطر أكثر، وزيادة التضييق في الاستهداف، بالمقارنة مع ما يكونه الحال عند جمع معلومات غير مشفّرة.

لنتذكر المبادئ الاقتصاديّة لـ «البيانات الضخمة» وهي: من الأسهل تجميع كل شيء بدل التفكير فيما يجب جمعه أو تركه، ومن الأسهل التجسّس على الجميع بدل التفكير في فرز من يستأهل التجسّس عليه. ويتكفّل انتشار التشفير بجعل عمليات الرقابة العامة غير مجدية، كما يفرض أن يقتصر التنصّت على أهداف منتقاة. وفي تلك الحال، تحقّق الخصوصيّة مكسباً كبيراً؛ لأن المُهاجِم لن يمتلك أبداً ميزانية تكفي لجعل الجميع أهدافاً منتقاة.

الثغرات وانتشارها

الثغرات أخطاء. أخطاء في تصميم النُظُم الإلكترونيّة أو تنفيذها- هنّات في الشيفرة أو المكوّنات الإلكترونيّة الصلبة - يتيح الدخول غير المصرّح به إلى النظام. بوسع مجرم في الفضاء السبراني، مثلاً، استغلال ثغرة ما ليدخل إلى حاسوبك، أو يتنصّت على اتّصالاتك الشبكيّة، أو يسرق كلمة المرور التي تستعملها في الدخول إلى حسابك البنكي. وربما يتمكن موظّف حكومي أمني من استعمال ثغرة ما لاختراق شبكة منظّمة إرهابيّة أجنبيّة وإجهاض عملياتها، أو سرقة الملكيّة الفكريّة لشركات

أجنبيّة. وربما يستغل موظّف آخر ثغرة ما للتنصّت على منشقين سياسيّين، أو خلايا إرهابيّة، أو قادة حكومات معادية. كذلك قد يستغل الجيش ثغرة ما لشن حرب في الفضاء الافتراضي. تندرج تلك الأفعال كلها تحت تصنيف الاختراق الإلكتروني.

عندما يكتشف المرء ثغرة معيّنة، يستطيع استعمالها للدفاع أو الهجوم. ويُترجَم الدفاع بالاتصال بالشركة البائعة وتنبيهها إلى الثغرة كي تعالجها وتسدّها، وكذلك نشرها كي يتمكن المجتمع من التعلّم منها. يجري التعرّف إلى ثغرات كثيرة من قِبَل الشركات البائعة، وتعمد إلى معالجتها من دون إثارة ضجيج حولها. ويحدث التعرّف إلى هشاشات أخرى على يد البحّاثة والـ «هاكرز» الأخلاقيّين.

يترجم الهجوم باستغلال الثغرة لشن هجمات على آخرين. ويطلق على الثغرات غير المعلن عنها تعبير «ثغرات اليوم صفر»، بمعنى أن قيمتها تأتي من كونها ثغرات تمنح المُهاجِم فرصة شن هجمات لا يملك أحد دفاعاً ضدها. وبذا، يكون من المستطاع شن هجمات عالميّة مع الإفلات من العقاب. وفي نهاية الأمر، سوف تكتشف الشركة الصانعة ثغرة ما- ويعتمد وقت حدوث الاكتشاف على المدى الذي استُغِلّت به الثغرة- ثم تصدر برنامجاً لسدّ تلك الثغرة.

إذا كان المُهاجِم المكتشف للثغرة مجموعة عسكريّة أو شركة لصنع الأسلحة، فلسوف تُبقي أمرها سراً كي تبني سلاحاً سبرانيّاً يستند إلى تلك الثغرة. وإذا جرى استغلالها لمرات نادرة وبسريّة مناسبة، فإنها تبقى طويلاً طي الكتمان. وإذا لم تستعمل إطلاقاً، فستبقى سراً إلى أن يكتشفها طرف آخر.

يستطيع مكتشفو الثغرات بيع معلوماتهم عنها[46]. هناك سوق قوي للأسلحة السبرانيّة المناسبة لـ «اليوم صفر»[47]- يتمثّل الشراة فيه بالحكومات والشركات التي تصنع الأسلحة السبرانيّة وتبيعها للحكومات[48]- إضافة إلى سوق سوداء يبيع فيها مكتشفو الثغرات المعلومات لمجرمين[49]. هناك شركات تمنح مكافآت

لمن يكتشـف ثغرات في منتجاتها بهدف تحفيز البحـوث الدفاعية، لكن الجوائز تبقى أقل مما يمكن تحصيله من بيعها.

مـن الأمور الشـائعة وجود ثغرات تصلح في «اليوم صفـر». إذ تحتوي كل قطعة من البرامج الرقميّة التجاريّة- في هاتفك الخلوي، وحاسـوبك المنزلي، والنُظُم التي تديـر المفاعلات الذريّـة- مئات بل آلافاً مـن الثغرات معظمها غير مكتشـف[50]. يرجـع ذلك إلى أن علم البرمجة ليس على قدر من التطوّر كي يعطي برامج خالية من العيوب كليّاً، وليس من المتوقّع أن يتغيّر ذلك الأمر قريباً. وتعطي اقتصاديات صنع البرمجيّات الرقميّة الأولوية إلى السرعة والميّزات الجذّابة، وليس للأمن[51].

المعنـى المقصـود من الـكلام هـو أن الاختراق لن يختفـي. في المسـتقبل المنظور، سـيكون من المسـتطاع دوماً أن يكتشـف مُهاجِم متمـرس تقنيّاً ثغرة كـي ينفذ منها إلى نظام المُدافع. ويصح ذلك أيضاً بالنسـبة للجيوش التي تصنع أسـلحة سـبرانيّة، ووكالات الاسـتخبارات التـي تحاول اخـتراق النُظُم الإلكترونيّـة بهدف التنصّت، وكذلك المجرمين من الأنواع كافة.

الحفاظ على إنترنت غير آمنة

في الفصـل الأول، بيّـنـتُ أن «وكالة الأمـن القومي» تخترق النُظُم الإلكترونيّة باسـتخدام ثغـرات موجـودة، وأخرى يجـري اصطناعها لتلـك الغايـة. وفي أفعال الوكالـة، تتقـدّم الرقابـة على الأمن، مـا يؤول إلى وضع نكـون فيه جميعاً أقـل أماناً. ويبـيّـن مقـال عن وثائق سـنودن نشرته صحيفة **الغارديان** البريطانيّة طريقة تفكير «وكالـة الأمن القومـي» ونظيرتها البريطانيّـة «القيادة الحكوميّـة للاتّصالات»[52]. ويورد المقال: «هناك ملخّصات متبادلة بين الوكالتين تظهران احتفالهما بهزيمة الأمن والخصوصيّة على الشبكة...».

كيف تقهر الحكومات الأمن والخصوصيّة معاً؟ بتنا نعرف أنّ «وكالة الأمن القومي» تستخدم 4 ممارسات رئيسة في عملها[53]. والأرجح أن دولاً كروسيا والصين وبلدان أخرى تفعل أموراً مُشابهة. وليس مجرمو الإنترنت ببعيدين عن ذلك أيضاً.

تعمد الوكالة إلى مراكمة الثغرات في البرامج الرقميّة التجاريّة التي نستخدمها يوميّاً، بدلاً من سعيها للتأكّد من إصلاح تلك الأخطاء. عندما تكتشف «وكالة الأمن القومي» (أو تشتري) ثغرة ما، فإنّها تستطيع إما أن تنبّه الشركة البائعة لتلك البرامج مع إصلاح تلك الثغرة غير المعروفة، أو تتمسّك بتلك الثغرة كي تكون منفذاً لها للتنصّت على نُظُم كومبيوتر تسعى الوكالة إلى استهدافها. ويخدم التكتيكان كلاهما أهدافاً مهمّة في سياسة الولايات المتّحدة، لكن يجب على الوكالة في كلّ مرّة أن تختار سلوك أيٍّ من الطريقين.

حاضراً، تملك الولايات المتّحدة- «وكالة الأمن القومي» والحكومة معاً- أعداداً متراكمة من ثغرات «اليوم- صفر»؛ ليس معروفاً عددها. في العام 2014، حاول البيت الأبيض توضيح ذلك الأمر بواسطة مُدوّنة إلكترونيّة، لكن ما قدّمه لم يكن شرحاً كافياً[54]. نعرف أن سلاحاً سبرانيّاً هو فيروس «ستاكس نت»، استخدم ذخيرة من ثغرات «اليوم- صفر» تكفي أربعة أيام من الحرب السبرانيّة[55]. ويؤشّر استخدام ذلك العدد في شنّ هجمة سبرانيّة مفردة على وجود ذخيرة لمئات الأيام في مخازن الحكومة.

في شهادته أمام الكونغرس، قدّم مايكل هايدن، المدير السابق لـ «وكالة الأمن القومي» تعريفاً لمصطلح متداول في أوساط الوكالة هو «نوباس» (NOBUS)[56] الذي يتألّف من الحروف الأولى لعبارة «لا أحد سوانا» بالإنكليزيّة (no body but us)- وهي إشارة إلى اكتشاف ثغرة يرجح ألا يعرفها أحد سوى الوكالة. تملك الوكالة آليّة سريّة كي تقرّر ما يجب فعله بصدد الثغرات. إذ تزعم الوكالة أنها

تعلن وتسدّ معظم ما تكتشفه من ثغرات[57]، لكنها تحتفظ ببعضها- وعددها غير معروف- عندما تتوصل إلى قناعة بأنّها ثغرة من نوع «نوباس».

تبدو تلك المقاربة كأنها تصلح إطاراً عاماً، لكنها تصبح صعبة عند التطبيق. من يعمل في حقل الأمن يعي صعوبة اتّخاذ قرارات من نوع «نوباس»، بل ربما لا تستطيع الحكومة ذلك أيضاً[58].

تحمل تلك السجلات المتراكمة للثغرات تهديداً للجميع. إذ تجعلنا الثغرات المفتوحة أقل أمناً، فلربما توصل أحد إلى معرفة إحداها واستخدمها في شنّ هجمات علينا. والأصل في تلك الثغرات أنها مزعزعة للاستقرار[59]، خصوصاً أنها لا تستمر طويلاً، فلا تحصل فائدة من مراكمة سجلات عنها والتفكير بأنها موجودة دوماً بتصرّفنا. والأنكى من ذلك كله أن كل استخدام لها يمتزج بخطورة أن يتنبّه آخرون لها ويسخّروها لمصلحتهم. ولأن تلك الثغرات تأتي في أنواع متراصفة، فإن حفظ السرّ بشأن إحداها ربما يعني أن صنفاً بأكمله من الثغرات يبقى غير مكتشف، وتالياً لا يجري سدّه وإصلاحه. وكذلك تكون الولايات المتّحدة والبلدان الأوروبيّة معرضة تماماً لتهديدات من نوع «اليوم- صفر»، بأثر من حساسيّة بنيتها التحتيّة الإلكترونيّة، والملكيّة الفكريّة والثروات الشخصيّة. وتكون بلدان كالصين وروسيا أقل تعرّضاً لتلك المخاطر- وكوريا الشماليّة أقل كثيراً-، لذا تتدنى لديهم كثيراً الحوافز للتصدي للثغرات والعمل على إصلاحها.

تعمل «وكالة الأمن القومي» على زرع «أبواب خلفيّة» في مُكوّنات الأجهزة الإلكترونيّة وبرامجها أيضاً. ليست «الأبواب الخلفيّة» شيئاً جديداً[60].

ولطالما أعربت شركات المعلوماتيّة والاتّصالات المتطوّرة عن قلقها حيال تمكن الـ «هاكرز» من زرع «أبواب خلفيّة» في البرامج، كما بذلت جهوداً ضخمة في العثور عليها وإزالتها. وأخيراً، صرنا نعرف أن الحكومة الأميركيّة تتعمد زرع «أبواب خلفيّة» في الأجهزة الإلكترونيّة والبرامج الرقميّة[61].

إذ تبينّ إحدى وثائق سنودن تفاصيل مشروع لـ «وكالة الأمن القومي» يحمل اسم «مشروع تمكين سيغينت» (SIGINT Enabling Project) [62] الذي يعتمد تكتيكات من قبيل «زرع ثغرات في نظم التشفير التجاريّة، ونُظُم المعلوماتيّة، والشبكات الرقميّة، والأجهزة الإلكترونيّة للاتّصالات التي يستخدمها الجمهور». لا يُعرَف الكثير عن ذلك المشروع، ولا عن مدى معرفته من قِبَل شركات صناعة المعلوماتيّة والاتّصالات المتطوّرة وموافقتها عليه، وكذلك الحال بالنسبة للسريّة التي تدسّ بها خلسة تلك الثغرات، سواء عبر موظفين في الشركات يعملون لمصلحة الحكومة أم بالتلاعب بطرق خفيّة بالشيفرات الرئيسة للشركات. وكذلك نجهل مدى نجاح المشروع- إذ لم تورد وثائق سنودن تفاصيل كثيرة عن ذلك- لكننا بتنا نعرف أنّ ميزانيته هي 250 مليون دولار سنويّاً. ولا نعرف أيضاً إذا كانت دول أخرى تفعل أشياء مشابهة بالنسبة للنُظُم التي تنتجها شركات تقع تحت سيطرتها السياسيّة.

لكن بعض الأمثلة باتت معروفة. في الفصل 6، تحدّثتُ عن تجاوب «مايكروسوفت» مع طلب «وكالة الأمن القومي» توهين شيفرة برنامج «سكايب». كذلك ضغطت الوكالة على «مايكروسوفت» لوضع «باب خلفي» في شيفرة برنامجها الذي يشغّل القرص الصلب «بيت لوكر» (Bit Locker) [63]. ومن المستطاع الافتراض بأن جهوداً أخرى طاولت منتجات أخرى، إذ تناهت إلى مسامعي بصورة شخصيّة بعض القصص عن إخفاقات في ذلك الصدد.

تحمل الثغرات المتعمّدة مخاطر كبرى، فلا وسيلة للتأكّد من أن «باباً خلفيّاً» دسّته الحكومة عمداً سوف يبقى حكراً عليها[64]. وتدفع ثغرات النفاذ المفروضة حكوميّاً بالشركات إلى جعل منتجاتها وخدماتها أقل أماناً بالنسبة للجميع[65].

مثلاً، بين حزيران (يونيو) 2004 وآذار (مارس) 2005، تمكن أحدهم من تتبّع مكالمات قرابة 100 خلوي لموظفين في الحكومة اليونانيّة، بينهم رئيس الوزراء، ووزراء الدفاع والخارجية والعدل، إضافة إلى مواطنين يونانيّين بارزين.

لقـد صمّمت شركة «إريكسـون» السـويديّة الشيفرة التي تمكّن من ذلـك التتبّع في منتجـات لشركة «فودافون»، لكنهـا لم تكن تُفَعّلها إلا للحكومات التي تطلب تلك المنتجـات[66]. لم تكـن الحكومـة اليونانيّة بين تلك الحكومات، لكـنّ أحداً ما- ربما مجموعة سياسيّة مناوئة أو تنظيم إجرامي- تمكّن خفية من تفعيل تلك الميّزة.

لم يكـن ذلـك حادثاً معزولاً. إذ حدث أمر مشـابه في إيطاليـا في 2006 [67]. في العـام 2010، اسـتفاد «هاكرز» صينيّون مـن ثغرة وضعها «غوغـل» عمداً في بريد «جـي ميل»، لتمكين الحكومة الأميركيّة من اعتراض الرسـائل الإلكترونيّة في ذلك البريـد[68]. وفي 2012، ظهر إلى العلن أن كل محـّول للاتصالات التليفونيّة بيع إلى وزارة الدفـاع، يحتـوي ثغرات مبثوثة في نظامـه للرقابة، لكن لم يكـن واضحاً مدى التعمّد في ذلك الأمر[69].

باسـتمرار، تسـتفيد «وكالة الأمن القومي» من «أبواب خلفيّـة» وضعتها بلدان أخرى في نُظُم إلكترونيّة، خدمة لأهداف أخرى[70]. ومثلاً، اسـتفادت الوكالة من قدرات في التتبّع وضعتها حكومة «برمودا» في نظامها الهاتفي، فتمكّنت الوكالة من تتبـع المكالمات الهاتفية *كافة* في ذلك البلد[71]. لَمَ نعتقد بأن ذلك لا يحصل للولايات المتّحدة أيضاً؟

تعمـد الوكالـة إلى تخريـب الجـداول الخوارزميّة ومعايـير التشـفير. هناك هدف آخر لـ «مشروع تمكين سـيغينت» يتمثّل في «التأثير في السياسـات، والمعايير والنُظُم المُحــدِّدة لتقنـيّات المفتـاح العام التجاري في التشـفير»[72]. ومرّة أخرى، لا تتوافر تفاصيل كثيرة عن تلك النشـاطات، لكني أتوقّع أنها تركز على المعايير المرسـومة في بـراءات اختراعات، كتلـك التي تحوزها شركات صنع الهواتـف الخلوية، بأكثر من تركيزها على معايير عامة كالجداول الخوارزميّة اللازمة للتشفير.

ومثـلاً، أثّـرت «وكالة الأمن القومـي» في تبني خوارزميّة توضـع في الخلويات من النوع الثاني المعروف باسم «جي إس إم» (GSM)، كي تتمكن من اختراقها بسهولة[73].

وهناك مثل معروف بشكل واسع هو أن الوكالة زرعت «باباً خلفيّاً» في محرّك مهمّته توليد الأرقام العشوائية المتعلّقة بعمليات تبادل البيانات والمعاملات بواسطة الإنترنت، ثم ضغطت كي يجري تبني ذلك المحرّك على نطاق واسع[74]. وترمي تلك الجهود لتوهين التشفير الذي يستخدمه الجمهور لحماية الاتّصالات بواسطة الإنترنت وعمليات البحث عن المعلومات في تلك الشبكة، لكنها جهود لم تكلّل بالنجاح.

في الفصل الخامس، تناولت ظهور «مجموعة عمليات الدخول المنسّقة» (اسمها المختصر «تاو») التابعة لـ «وكالة الأمن القومي»، وهي مختصّة في اختراق الإنترنت. وإضافة إلى عمليات الاختراق المباشر للحواسيب وأجهزة صنع الشبكات الرقميّة، تنكّرت الوكالة على هيئة مواقع كـ «فيسبوك» و«لينكدن» (وربما مجموعة من المواقع الشبكيّة الأخرى)[75]، لتخترق حواسيب معيّنة، ولتوجّه الحركة الإلكترونيّة في الموقعين (وربما مواقع أخرى) إلى مواقع مزيّفة أنشأتها الوكالة بهدف التجسّس على الجمهور. وكذلك تستطيع «قيادة الاتّصالات المركزية» في المملكة المتّحدة أن تعثر على صورك الحميمة في «فيسبوك»، وترفع بشكل زائف أعداد زوّار موقع معيّن، وتعبث في تسجيلات الفيديو في موقع ما، وتمحو حسابات بأكملها من الإنترنت، وتسطو على استطلاعات الرأي وأكثر من ذلك بكثير[76].

وإضافة إلى انعدام الثقة العميق الذي تولّده تلك الممارسات في صفوف جمهور الإنترنت، فإنها تفرض على «وكالة الأمن القومي» ضمان أولويّة الرقابة على حساب الأمن. وبدلاً من تحسين أمن الإنترنت لمصلحة الجميع، فإنّ ما تفعله الوكالة فعليّاً هو ضمان بقاء الإنترنت غير آمنة؛ خدمة لمصالح الوكالة واستمرارية قدرتها على اختراق تلك الشبكة.

يتسبّب ذلك بالأذيّة لنا جميعاً؛ لأن الوكالة ليست الطرف الوحيد الذي يستفيد من زعزعة الأمن الشبكي. هناك حكومات وتنظيمات إجراميّة تستفيد من ذلك أيضاً. وهناك عدد مدهش من تقنيّات الاختراق على الإنترنت ليست حكراً على «وكالة الأمن

القومي»، وفق ما بيّنته وثائق سنودن، بل إنها ليست حكراً على أجهزة الاستخبارات التابعة للدول أيضاً. إنّها تقنيّات اختراق برسم من يدفع بسخاء لشرائها[77]. وناقش بعض الأكاديميّين إمكان إعادة صنع تقنيّات تستخدمها الوكالة لجمع البيانات وتحليلها، بواسطة نُظُم مفتوحة المصدر لوضعها بتصرف الجمهور مجاناً، وكذلك إتاحة تلك التقنيّات للشركات التي تصنع النُظُم الرقميّة التجاريّة أيضاً[78].

ومثلاً، عندما كنتُ أعمل في صحيفة الغارديان البريطانيّة، استماتت «وكالة الأمن القومي» كي تمنعنا من كشف برنامج معين كانت تعتبره فائق السريّة، ويحمل اسم «كوانتوم» (Quantum)[79]. ويتعلّق عمل البرنامج بتقنيّة اسمها «حقن الباكيت»(*) (Packet Injection)، وهي أساساً تقنيّة تتيح للوكالة اختراق الكومبيوتر[80]. وبالنتيجة، تبيّن أن الوكالة لم تكن الطرف الوحيد الذي يستخدم تلك التقنيّة. إذ تستخدم الحكومة الصينيّة تقنية «حقن الباكيت» لمهاجمة الحواسيب[81]. وتبيع شركة «هاكنغ تيم»، المختصة بصنع أسلحة الفضاء الافتراضي، التقنية عينها لأي حكومة ترغب في الدفع بسخاء لشرائه[82].

كذلك تستخدم تلك التقنية منظّمات إجراميّة عدّة. وهناك أدوات تقنية لاختراق الكومبيوتر موضوعة بتصرّف الأفراد[83]. كانت تلك الأشياء جميعها موجودة عندما كتبتُ عن تقنية «كوانتوم». وباستعمال معرفتها لمهاجمة الآخرين، بدلاً من بناء نظام دفاعي على الإنترنت، أدّت أعمال الوكالة إلى وضع تقنية «حقن الباكيت» في يد كل من يقدر على دفع ثمنها ليستعملها في اختراق الحواسيب.

وحتى عندما تبتكر تقنيّات داخل «وكالة الأمن القومي»، فإنّها لا تبقى حكراً على الوكالة لفترة طويلة[84]. إذ إنّ البرامج السريّة اليوم تصبح غداً موضوعاً لرسالة دكتوراه، ثم تتحوّل أداة في يد الـ «هاكرز» في اليوم التالي. وهناك مثل عمليّ

(*) تتحرّك البيانات على الإنترنت ضمن رزم محدّدة تشبه المقطورات في قطار طويل. وتسمى كل مجموعة (أو مقطورة) "باكيت"، وتتبع تسلسلاً رقميّاً معيّناً، يربطها بالبقية، ما يضمن استمرارية حركة البيانات.

على ذلك: استعملت تقنيّات عسكريّة مخصّصة للحرب الافتراضيّة في صنع فيروس «ستاكس نت»، وسرعان ما صارت أدوات في أيدي عصابات الجريمة المنظّمة. وهناك برامج رقميّة لكسر كلمات المرور باعتها شركة «إلكومسوفت» (Elcomsoft) للحكومات، وسرعان ما استخدمت لاختراق السحابة المعلوماتيّة التابعة لشركة «آبل» والمسمّاة «آي كلاود» (iCloud) وسرقة صور المشاهير[85]. وما كانت ذات مرّة برامج سريّة لمراقبة خلويات الأفراد، صارت الآن سلعة شائعة الاستعمال[86].

تأثّر عمل الإنترنت كثيراً برغبة الحكومة الأميركيّة في ممارسة رقابة غير مقيّدة على تلك الشبكة. وعندما تضحي الرقابة عملاً تعاونيّاً بين حكومات عدّة، تتفوق متطلّبات ذلك الوضع على المعطيات الأخرى كافة. ويعمد مهندسو الشبكات إلى تبني تصاميم تتجاوب مع حاجات الرقابة لدى الحكومات، وتستمر تلك التصاميم لعقود طويلة ببساطة؛ لأنّه من الأسهل الاستمرار في عمل الأشياء عينها، بدل الإقدام على التغيير. وبإعطائها الأولويّة للرقابة على حساب الأمن، ضمنت «وكالة الأمن القومي» أن نكون جميعاً غير آمنين.

أضرار جانبيّة من الهجمات السبرانيّة

مع استمرار الاختراقات المتبادلة بين الأمم على الإنترنت، يصبح جمهورها جزءاً من أضرارها الجانبيّة باطّراد. في أغلب الأحيان، لا نعرف التفاصيل، لكن أحياناً تطفو على السطح بعض المعلومات عن مدى الضرر الذي يلحق بنا.

هنالك 3 أمثلة على ذلك. أولاً، استهدف الفيروس الإلكتروني «ستاكس نت» إيران[87]، لكن حدث أن الفيروس تسرّب إلى ما يزيد على 50 ألف كومبيوتر في الهند وأندونيسيا وباكستان وغيرها، من بينها حواسيب تملكها شركة «شيفرون»[88] وشركات صناعيّة ألمانيّة[89]، ولربما تسبّب أيضاً في سقوط قمر اصطناعي هندي في 2010 [90]. يزعم سنودن أن «وكالة الأمن القومي» تسبّبت خطأً في قطع الإنترنت عن سوريا في 2012 [91]. وعلى نحو مُشابِه، يستخدم «سور النار العظيم» الرقمي

في الصين، تقنية تسـمّى «حَقن نظام أسماء النطاق»(*) (Domain Name System)، لمنع الوصول إلى مواقع معيّنة؛ وهي تقنيّة تؤدّي إلى اضطراب في حركة الاتّصالات بواسطة الإنترنت، حتى تلك التي لا تتصل بالصين ولا المواقع الممنوعة[92].

كلما زادت الاختراقات المتبادلة بواسطة الإنترنت بين الأمم، سواء لإحداث ضرر أم للحصول على معلومات استخباراتيّة، أضحت الشبكات الرقميّة المدنيّة أكثر عرضة لأن تتحوّل إلى مجرد ضرر جانبي.

تضرّر المصالح الوطنيّة

في الفصل 9، ناقشت الضرر الذي تلحقه نشاطات «وكالة الأمن القومي» باقتصاد الولايات المتّحدة، إضافة إلى إلحاقها الضرر بالمصالح السياسيّة لأميركا.

وناقش عالِم السياسة أيان برمر أن ما كشُف للعموم عن نشاطات «وكالة الأمن القومي» أدى إلى «الإساءة بشدّة إلى مصداقيّة الولايات المتّحدة لدى كثيرين من حلفائها»[93]. وعلى المسرح الدولي، تأذّت مصالح الولايات المتّحدة بعمق، إذ علمت دولة تلو الأخرى عن تلصص أميركا على قادتها[94]. شمل ذلك بلداناً صديقة في أوروبا وآسيا وأميركا اللاتينيّة. وبصورة خاصة، تأذّت العلاقات بين أميركا وألمانيا عندما كُشِفَ علانية أن «وكالة الأمن القومي» تجسّست على هاتف المستشارة الألمانيّة أنغيلا ميركل[95]. وكذلك تجاهلت الرئيسة البرازيليّة ديلما روسيف دعوة إلى عشاء عمل في الولايات المتّحدة- وهي المرّة الأولى لرئيس برازيلي- بسبب الغضب الذي شعرت به روسيف وبلادها من رقابة الوكالة[96].

تحدث أشياء أكثر من ذلك كثيراً خلف الستار، وتمر بأقنية دبلوماسيّة شديدة الخصوصيّة. إذ لا مجال للتعامل برقّة مع تخريب الولايات المتّحدة علاقاتها وموقعها وقيادتها الدولية، بأثر من برنامجها الشرس في الرقابة.

(*) يعمل "نظام أسماء النطاق" على الربط بين الاسم الفعلي لصاحب الكومبيوتر، وهوية الحاسوب الإلكترونيّة المؤلّفة من سلسلة أرقام تُعطى له عند الانتهاء من صنعه.

الجزء الثالث

كيف نتصرف بشأنها؟

12

المبادئ

تتعدّد الأضرار الناجمة عن الرقابة العامة، وتتجاوز كلفتها على الأفراد والمجتمع بأشواط ما تقدّمه من منافع. يجب على الجميع فعل شيء ما للسيطرة عليها، بل إنّهم يقـدرون على ذلك. وقبل التقدّم باقتراحات محـدّدة تقنيّاً وقانونيّاً واجتماعيّاً، أود أن أستهل الفصل ببعض المبادئ العامة. وتمثّل المبادئ حقائق شاملة عن الرقابة وكيفيّة التعامل معها، كما تنطبق على الحكومات والشركات معاً.

يشـكّل تجميع المبادئ الجزء السـهل من الموضوع؛ فيما الأصعـب هو تطبيقها في أوضاع محدّدة. «الحياة والحريّة والبحث عن السعادة» هي مبادئ نُجمِع عليها، لكن مجرد إلقاء نظرة على مسار الأمور في العاصمة واشنطن، تكفي لإظهار مدى صعوبة تطبيقها. حضرت نقاشات ومنتديات حوار كانت الأطراف المختلفة فيها متّفقة على المبادئ العامـة بخصوص جمع البيانات والرقابـة والإشراف والأمن والخصوصيّة، لكن ذلك لم يحل دون اختلافها بشدّة حول طرق تلك المبادئ في الواقع فعليّاً.

الأمن والخصوصيّة

غالبـاً ما يوصف ذلـك الضرب من النقاش بعبارة «الأمـن مقابل الخصوصيّة». تمـلي علينـا تلك الرؤية المبسّـطة أن نجـري نوعاً مـن المقايضة المبدئيّة بـين الأمرين، بمعنـى أنه كي نكـون آمنين يجب أن نُضحّـي بخصوصيّتنا ونستسـلم للرقابة. وإذا

أردنا مستوىً معيّناً من الخصوصيّة، يجب أن نقرّ بضرورة التضحيّة بجزء من أمننا للحصول عليه.

إنّها مبادلة زائفة. أولاً، يصح القول إن بعض إجراءات الأمن تتطلّب من الناس تخلياً عن الخصوصيّة، لكن بعضها الآخر لا يمسّ الخصوصيّة كليّاً؛ كأقفال الأبواب، السياجات المرتفعة، الحرس، الأبواب المحصّنة لقمرة القيادة في الطائرة، وغيرها. وثانياً، من الناحية المبدئيّة، ثمة تحالف بين الخصوصيّة والأمن. عندما نفقد الخصوصيّة، نشعر بأننا مكشوفون وعرضة للخطر؛ نشعر بأمن أقل. وكذلك عندما تكون مساحاتك الشخصيّة وسجلاتك غير آمنة، تمتلك خصوصيّة أقل[1]. يتحدّث التعديل الأساسي الرابع في الدستور الأميركي عن «حق الناس في أن يكونوا *آمنين* في أشخاصهم وبيوتهم وأوراقهم وممتلكاتهم الشخصيّة المنقولة» (التشديد من المؤلّف). وأقرّ واضعو الدستور بأن الخصوصيّة ركن أساسي في أمن الأفراد.

لذا، يؤدّي صوغ النقاش على هيئة مبادلة بين الأمن والخصوصيّة إلى تقويمات منحرفة. وفي أغلب الأحيان، تصاغ تلك المبادلة في صيغة الكلفة الماليّة: «كم تدفع من أجل الخصوصيّة»؟ أو «كم تدفع للحصول على الأمن»؟ لكن ذلك يمثّل مبادلة زائفة أيضاً. إنّ تكاليف انعدام الأمن حقيقيّة وعميقة، حتى كفكرة مجرّدة. وكذلك فإن تكاليف انعدام الخصوصيّة واضحة وجلية كفكرة مجرّدة، وتغدو ملموسة بمجرد أن يفتقدها المرء ويعاني تأثيرات غيابها. وللسبب عينه، لا نعطي للخصوصيّة مكانتها المستحقّة عندما نمتلكها، ولا نفهم قيمتها فعليّاً إلا عندما نفقدها. وللسبب عينه، نسمع من يقول إن الناس غير مستعدّة لأن تدفع مقابل خصوصيتها، وإن الأمن يتفوّق على الخصوصيّة بالمطلق.

عندما تُصاغ مبادلة الأمن بالخصوصيّة على شكل خيار بين الحياة [الأمن] والموت، ينتهي النقاش العقلاني كليّاً[2]. كيف يمكن للمرء أن يتحدّث عن الخصوصيّة عندما تكون حياة الناس على المحك؟ إذ يكون الناس المذعورون أشد

استعداداً للتضحية بخصوصيّتهم مقابل الشعور بالأمن. ويفسّر ذلك سبب إعطاء الحكومة الأميركيّة سلطة مطلقة في فرض رقابة عامة عقب هجمات الإرهاب في 9/ 11. إذ قالت الحكومة أساساً[3] إنّه يجب علينا جميعاً أن نتخلى عن خصوصيّتنا مقابل الأمان؛ ولم تكن لغالبيتنا معرفة بخيار أفضل، ولذا قبلت بتلك المبادلة الفاوستيّة(*).

تتمثّل المشكلة في أن الوزن الكامل لانعدام الأمن يوضع في الكفة المقابِلَة للغزو التدريجي للخصوصيّة. تفعل محاكم أميركا ذلك، قائلة أشياء من نوع «نقرّ بأنّ هناك خسارة للخصوصيّة في برنامج حكومي أو آخر، لكن ثمن تفجير قنبلة ذريّة في نيويورك، يفوق ذلك بكثير». إنّه تمثيل ضبابيّ للمبادلة. وليست المسألة أن تفجيراً نووياً يغدو مستحيلاً إذا خضعنا للرقابة جميعاً، ولا أنه يصبح قدراً لا مفر منه إذا لم تحدث تلك الرقابة. الحال أن احتمال حدوث ذلك هو ضئيل فعليّاً، ولا يؤدي غزو برنامج الأمن للخصوصيّة، إلى خفضه نظريّاً إلا بقدر فائق الضآلة. إذاً، يجب إعادة النظر في المبادلة.

وعلى وجه العموم، يجب ألّا يكون هدفنا هو البحث عن مبادلة مقبولة بين الأمن والخصوصيّة؛ لأنه من المستطاع [والواجب] الاحتفاظ بكليهما معاً سويّة[4].

تقدّم الأمن على الخصوصيّة

تتضارب متطلّبات الأمن والخصوصيّة. ويصعب مراقبة نظام صُمّم لغايات الأمن. وبالعكس، تصعب حماية نظام صُمّم لتسهُل رقابته. وتسدّد قدرات الرقابة المثبتة في نظام ما ضربة إلى أمنه؛ لأننا لا نعرف كيف نبني نظاماً لا يسمح بالرقابة إلا للأشخاص *الموثوقين* وحدهم. ونوقش ذلك في الفصل 11.

(*) إشارة إلى شخصيّة خياليّة هو الشاب فاوست الذي عقد صفقة مفادها أن يحتفظ بشبابه ووسامته إلى الأبد، مقابل بيع روحه إلى الشيطان.

لنلاحظ أيضاً أنّه بالنسبة للمجتمع ككل، يمتلك الأمن أهمية حاسمة أكثر من مسألة الرقابة. وبقول آخر، يجب علينا اختيار بنية تحتيّة للمعلومات تكون آمنة ومنيعة على الرقابة، بدلاً من بنية غير آمنة يسهل فرض رقابة عليها[5].

تنطبق تلك المحاججة على وجه التعميم. إذ يسهل استخدام بنيتنا التحتيّة في المعلومات، لأغراض سيّئة وجيّدة. يقود سُرّاق البنوك سيّاراتهم على الطرق السريعة، يستخدمون الكهرباء، يشترون أجهزتهم من المحلات الكبرى، ويتناولون وجباتهم في المطاعم التي تفتح على مدار الساعة، تماماً مثلما يفعل الناس الشرفاء. ويتشارك الأبرياء والمجرمون في استعمال الخلوي والبريد الإلكتروني والمخازن الشبكيّة من نوع «دروب بوكس» (Drop Box). ويهطل المطر على العادل والظالم معاً.

وعلى الرغم من ذلك، يستمر المجتمع في تدبّر أموره لأن الاستخدامات الشريفة والإيجابيّة والمفيدة للبنية التحتيّة تفوق كثيراً الاستخدامات السلبيّة والمؤذية وغير الشريفة. لا يمثّل سُرّاق البنوك سوى نسبة لا تذكر ممن يقودون سيّاراتهم على الطرقات السريعة، وكذلك الحال في نسبة المجرمين إلى إجمالي مستخدمي البريد الإلكتروني. ويبدو أكثر منطقيّة أن تبنى تلك النُظُم كلها كي تخدم غالبيتنا التي تحتاج إلى الأمن من المجرمين والمتسوّقين الشبكيّين الذين يسطون على حسابات الآخرين، بل من حكوماتنا أحياناً.

وعندما نضع نظاماً تراتبيّاً لأولويّات الأمن، نستطيع حماية تدفق المعلومات عالميّاً- بما فيه معلوماتنا وبياناتنا- من التنصّت والهجمات الأكثر إيذاءً كالسرقة والتخريب. وينفتح المجال لحماية تدفقات معلوماتنا من الحكومات والمجرمين واللاعبين غير الرسميّين. حينها، نجعل العالم أكثر أمناً ككل.

يعطي برنامج «تور» (Tor) مثلاً ممتازاً[6]. ويتميّز «تور» بأنه يعمل بنظام المصدر المفتوح المجاني، ويمكنك أن تستخدمه من أجل الإبحار على الإنترنت من دون

كشف هويّتك. جرى تطويره أصلاً بفضل تمويل من «مختبر البحوث» التابع للبحريّة الأميركيّة، ثم موّلته وزارة الخارجيّة. ويستخدمه المنشـقّون في العالم أجمع للنجاة من الرقابة والحجب. وبديهي القول إنه يسـتعمل أيضاً من قِبَل المجرمين للغاية نفسـها. ويعمـل صانعـو «تور» على تطويره باسـتمرار كي يقدر عـلى التملّص من محاولات الحكومـة الصينيّـة حظـره عـلى مواطنيها. ونعلـم أيضـاً أن «وكالة الأمـن القومي» حاولت كسر شـيفرته باسـتمرار[7]، لكنها فشـلت[8]، على الأقل وصـولاً إلى العام 2007 وفق ما بيّنته وثائق سـنودن. ونعلم أن الـ «إف بي آي» اسـتمرت في اختراق الحواسـيب في 2013 و2014؛ لأنهـا فشـلت في محاولة كسر شـيفرة «تـور»[9]. في الوقت نفسـه، نعتقد بأن أشـخاصاً عملوا لمصلحة «وكالة الأمن القومي» و«القيادة الحكوميّـة للاتّصـالات» البريطانيّة، يسـاعدون خفية في الحفاظ على شـيفرة «تور» وأمنهـا[10]. ويصـل بنا الكلام إلى مأزق: إما أن «تور» قـوي بما فيه الكفاية فيحافظ على خفاء من نريد ومن لا نريد، أو أنّه ضعيف فلا يحافظ على خفاء الطرفين كليهما.

بديهـي أنه لن يـأتي زمن خلو من التجسّـس. ويكـون سـذاجة الاعتقاد بعكس ذلـك. فمنذ بدايـة التاريخ، تلجأ الحكومات إلى التجسّـس[11]، بل ترد قصص عن التجسّـس في التوراة[12]. يبرز سـؤال فعلي عن نوع العالم الذي نصبو إليه. هل نريد فعليّـاً تخفيـف التفاوت في القـوى بالحد من قدرات الحكومة عـلى الرصد والحجب والتحكّم؟ أم إننا نسمح للحكومة بزيادة سلطتها علينا؟

«الأمـن يتقدّم على الرقابة» ليس قانوناً ثابتاً بالطبع. هناك أوقات تقتضي تصميم نظـام للحماية من تلك الأقلية غير الشريفة التـي تعيش بيننا. ويعطي أمن الطائرات مثلاً على ذلك، إذ لا يمثّل عدد الإرهابيّين بالنسـبة لإجمالي من يسـافرون جوّاً سوى أقليـة ضئيلة تمامـاً. وعلى الرغم من ذلك، تصمّـم المطـارات كلها حول فكرة الحماية من تلك الفئة الفائقة الصغر؛ لأن الفشل في الأمن على متن طائرة يؤدي إلى كوارث أكـبر كثـيراً من تفجـيرات القنابل الإرهابيّـة في أمكنة أخرى. في المقابـل، لا نصمّم مجتمعنا بأسره [ليس بعد] حول فكرة الحماية من الإرهاب[13].

كذلك هنالك أوقات نحتاج فيها لوجود رقابة ملائمة في النُظُم. إذ نرغب في أن تكون خدمات الشحن البحري قادرة على تتبّع الطرود في الوقت الحقيقي. نرغب أيضاً في أن يعرف من يردّون أولاً على الاتّصالات الطارئة، ومصدر تلك المكالمات. وبالطبع، لا نستعمل كلمة «رقابة» في تلك الأحوال، بل نلجأ إلى عبارات ملطّفة من نوع «تتبّع الطرود».

في تلك الأحوال، يبرز مبدأ عام مفاده أن النُظُم يجب أن تتبنى حدّاً أدنى من الرقابة يكون ضرورياً كي تستمر في العمل، إضافة إلى اكتفاء الرقابة حين تكون مطلوبة؛ بالحدّ الأدنى الضروري من المعلومات مع الاحتفاظ بها أقصر وقت ممكن.

الشفافيّة

الشفافيّة أمر ضروري لكل مجتمع حرّ ومنفتح. تتيح القوانين الحكوميّة المفتوحة وقوانين حريّة المعلومات للمواطنين معرفة ما تفعله الحكومة، كما تمكّنهم من إنجاز واجبهم الديمقراطي في الإشراف على نشاطاتها. وفي القطاع الخاص، تؤدي قوانين الصراحة في الشركات وظيفة مماثلة. بالطبع، تحتاج الحكومة والشركات معاً إلى شيء من السريّة، ولكن كلّما ازدادوا شفافيّة، استطعنا أن نقرّر عن معرفة مدى ثقتنا بهم[14]. وحتى الآن، تملك الولايات المتّحدة حكومة منفتحة تماماً مع قوانين لحرية المعلومات، لكن هناك معلومات كثيرة لا ينطبق عليها ذلك[15].

بالنسبة للمعلومات الشخصيّة، تكون الشفافيّة مباشرة إلى حدّ كبير: إذ يملك الناس الحق في معرفة المعلومات والبيانات التي جُمِعَت عنهم، كم ذهب منها إلى الأرشيف، كيف استُخدِمَت، ومِنْ قِبَل مَنْ. نكون ميّالين لارتياح إلى الرقابة بأنواعها، إذا أحطنا علماً بتلك الأشياء. يفترض بسياسات الرقابة أن تعطي الناس تلك المعلومات، بدل تعمّد إدخالها في ضبابيّة تُفقِدها القدرة على إنارة الأمور.

نحتـاج أيضـاً إلى معرفة الخوارزميـات المؤتمتة التي يناط بهـا التوصّل إلى أحكام وخلاصات بشـأننا اسـتناداً إلى بياناتنا، إما بنشر شيفرة الخوارزميات أو بشرح وافٍ عـن طريقـة عملها. وحـاضراً، لا نسـتطيع الحكم على مـدى عدالـة الخوارزميّات التـي تسـتخدمها «أمن إدارة النقل» في إعداد قوائم مـن يجب إخضاعهم لـ «تفتيش مسـحي خـاص»[16]. وينطبق الأمر عـلى الخوارزميات التي تسـتخدمها «مصلحة المداخيـل الداخليّة» لانتقاء من يجب التدقيق في مداخيلهم[17]. وتتكرّر الحال عينها بالنسـبة للخوارزميات التي يستخدمها محرّك البحث للبتّ في شأن الصفحات التي يمكننا مشـاهدتها على الإنترنت؛ وخوارزميّات التوقّع الشُرَطي التي تحدّد من يجدر جلبـه للتحقيـق وما هي الأحيـاء التي يجب اسـتهدافها من قِبَل دوريـات الشرطة؛ وخوارزميـات الوضـع الائتماني التي تقرّر جدارة الأفـراد في الحصول على رهونات عقاريّة. هناك شيء من السريّة يفرض نفسه في تلك الأمور، لمنع الناس من التلاعب بالنظام، لكن الإكثار من السريّة ليس ضرورياً البتّة. ويتيح «قانون حماية المعلومات» في «الاتحاد الأوروبي»، الكشف عن جلّ تلك المعلومات.

أبدو كمن يتناقض مع نفسـه. من ناحية، أُناصر الخصوصيّة الفرديّة على حساب الرقابـة المفروضـة. ومن الناحيـة الثانية، أؤيّد تقديم شـفافيّة الحكومـة والشركات على حسـاب السريّة المؤسّسـاتيّة. ويكمن السـبب في تأييدي الأمرين معاً، في الخلل حاضراً في ميزان القوة بين الناس والمؤسّسات[18]. إذ تفوق قوّة المؤسّسات ما يملكه الجمهـور، ويتنامى الخلل باسـتمرار. وتعمل سريّة المؤسّسـات على زيـادة قوّتها، ما يزيـد الخلل أيضـاً. ويحمل الأمر تهديـداً أساسـيّاً للحريّة الشـخصيّة. كذلك تنمي الخصوصيّـة الفرديّـة قوّة الأفـراد، ما يخفف الخلل؛ وهو أمر مفيـد للحريّة. وينطبق الأمر تماماً على الشفافيّة والرقابة[19]. إذ تخفض الشفافيّة المؤسّساتيّة الخلل في القوّة، وهو أمر إيجابي[20]. وتزيد رقابة المؤسّسـات على الأفراد من الخلل، وهو أمر سـيئ تماماً.

لا تأتي الشفافيّة بسهولة[21]. ولا يرغب القوي في التدقيق به. ومثلاً، تبدي الشرطة نفوراً متزايداً من تقييمه. في الولايات المتّحدة بأكملها، تلاحق الشرطة وتضايق من يسجّلون أشرطة عنها[22]، بل إنّ سلطات قضائيّة عدَّت تلك الأشرطة غير قانونيّة[23]. ويتعمّد رجال الشرطة في شيكاغو تعمية الكاميرات، ما يظهر كأنه مسعى لإخفاء أفعالهم بالذات[24]. وترفض دائرة الشرطة في «سان دييغو» كل طلبات الحصول على أشرطتها، مصرّة على أنها جزء من تحقيقات جارية[25]. وخلال التظاهرات الاحتجاجيّة للعام 2014 في بلدة «فيرغسون» بولاية «ميسوري»، التي اندلعت إثر مقتل رجل أسود غير مسلح على يد الشرطة، حرصت الشرطة باستمرار على منع المحتجّين من تصويرها، واعتُقِل مراسلون كُثُر بسبب توثيق تلك الحوادث[26]. وذهبت الشرطة في «لوس أنجلوس» إلى حدّ تخريب التسجيلات الصوتيّة في سيارات دوريّاتهم، على الرغم من أن القانون يتطلّب وجودها.

وبصورة دائمة، تقاوم الحكومات والشركات قوانين الشفافيّة من الأنواع كافة. في المقابل، يتعرّض عالم السريّة للتبدّل. وكتب الباحث في قانون الخصوصيّة بيتر سواير عن التناقص المستمر في دورة حياة الأسرار[27]. ولاحظ أنّ الأسرار عموماً صارت تنكشف أسرع من العادة. وتجعل التكنولوجيا الأسرار أصعب حفظاً، وتصعّب طبيعة الإنترنت الاحتفاظ بها لزمن طويل. يكفي الضغط على زر «أرسل» إلى نشر غيغابايتات من المعلومات، بمثل لمح البصر. وفي كل سنة، تزيد قدرة مفاتيح الذاكرة الخارجيّة على تخزين المعلومات. وتحتاج الحكومات والشركات إلى افتراض أن أسرارها صارت أشد عرضة للانكشاف، وبسرعة كبيرة، أكثر من أي وقت مضى.

يترتب على تقاصر دورة حياة الأسرار نتائج منها أن انكشافها صار أكثر إيذاءً. أشارت إحدى وثائق سنودن إلى تجسّس «وكالة الأمن القومي» على هاتف المستشارة الألمانيّة أنغيلا ميركل[28]. لم تحمل الوثيقة تاريخاً محدّداً، لكنها ترجع بوضوح إلى سنوات قليلة خلت. لو كُشِفَت الوثيقة عينها بعد عشرين سنة من الآن، لكانت ردّة

الفعل عليها في ألمانيا مختلفة جداً عن الزمجرة العامة التي علَت في 2013، فيما ميركل لا تزال في مكتب المستشاريّة وتعلّق الأمر بحدث جارٍ، وليس حدثاً من التاريخ.

تصعّب التغيّرات الثقافيّة الجارية حاضراً الحفاظ على الأسرار. في الأيام الخوالي، كان الحفاظ على أسرار المؤسّسة جزءاً من ثقافة تستمر مدى الحياة. وكانت الاستخبارات توظّف أشخاصاً في مقتبل العمر، وتسند إليهم وظائف تستمر طيلة حياتهم. كانت أشبه بنادٍ خاص يحتكره الرجال، ومملوء بالكلمات المشفّرة والمعرفة السريّة[29]. وكذلك كان عالم الشركات مكتظاً بمن يعملون مدى الحياة. خلت تلك الأيام. هناك وظائف كثيرة في عالم الاستخبارات يجري تعهيدها إلى أطراف تعمل خارجه، ولم يعد مفهوم «وظيفة مدى الحياة» موجوداً في عالم الشركات. صارت قوى العمل مطواعة، والوظائف قابلة للتعهيد، والأشخاص قابلين للاستبدال. بات العُرف السائد هو الانتقال من رب عمل إلى آخر[30]. ويعني ذلك أن الأسرار يجري تشاركها بين عدد أكبر من الناس الذين يتدنى اهتمامهم بالحفاظ عليها. لنتذكّر أن خمسة ملايين شخص في الولايات المتّحدة يحملون أُذونات أمنيّة، وأنّ معظمهم متعاقدون وليسوا موظّفين حكوميّين[31].

هناك إيمان متصاعد بقيمة الانفتاح، خصوصاً في أوساط الشباب. ويبدي الأصغر سناً ارتياحاً أكبر للتشارك في المعلومات الشخصيّة، بالمقارنة مع من هم أكبر سنّاً[32]. إذ يؤمن الشباب أن المعلومات يجب أن تكون حرّة، والأمن يأتي من انتشار المعرفة بين العموم، إضافة إلى النقاشات بينهم. يعبّر الشباب عن أشياء شخصيّة على الإنترنت، كما نشروا بأنفسهم صوراً محرجة لهم على مواقع شبكات التواصل الاجتماعي. وهجرهم من يحبونهم علانية في المنتديات الشبكيّة. تشارك الشباب بأشد الطرق إرهاقاً، لكنهم اجتازوا ذلك بسلام. من الصعوبة بمكان الترويج في صفوف ذلك الحشد الشبابي، أن حق الحكومة في السريّة يتقدّم على حق الناس في المعرفة[33].

إنّها ميول تكنولوجيّة واجتماعيّة جيّدة. يجب النضال من أجل الشفافيّة، كلما أمكن ذلك[34].

الإشراف والموثوقيّة

من أجل استمراريّة معظم المجتمعات، يجب على الناس أن يعطوا لآخرين سلطة عليهم. يتضمّن التنازل عن السلطة شيئاً من الخطورة بشكل لا مفر منه، وعلى مدار آلاف السنوات، طوّر البشر أُطُراً لحماية أنفسهم من تنازلهم عن السلطة لفئة منهم، وهي تشمل الشفافيّة والإشراف والموثوقيّة. إذا عرفنا كيف يستخدم الآخرون السلطة التي منحناها لهم بأنفسنا، نستطيع أن نضمن لأنفسنا أنهم لن يسيئوا استخدامها؛ وإذا قدرنا أن نعاقبهم عندما يسيئون، نستطيع أن نثق بهم أكثر عندما نعطيهم السلطة. يمثّل ذلك عقداً أساسيّاً في الديمقراطيّة.

هناك مستويان من الإشراف. هناك أولاً الإشراف الاستراتيجي الذي يلخّصه السؤال عن مدى صحة القوانين التي نتبنّاها. ومثلاً، تستطيع «وكالة الأمن القومي» تنفيذ إجراءاتها الخاصة كي تتأكّد من اتّباعها القانون، لكن يجب ألا تقرّر القوانين التي يجب عليها اتّباعها. شرِحَ ذلك بطريقة حسنة تماماً منْ قِبَل مايكل هايدن، المدير السابق لـ «وكالة الأمن القومي»: «أعطني حدود الصندوق الذي تسمح لي بالعمل ضمنه، ولسوف ألعب حتى الحدود القصوى للصندوق... أنتم، الشعب الأميركي، أعطوني بواسطة ممثليكم المنتخبين حقلاً للعب، ولسوف ألعب بكل قسوة فيه»[35]. هناك معنىً واحد تصح فيه هذه الأقوال: ليست وظيفته أن يسنّ القوانين، لكنه مخطئ في كل معنىً آخر، وهو ما سأشرحه في الفصل 13.

في الحالين، يجب أن نتحسن في شأن الإشراف الاستراتيجي. نحتاج إلى نقاشات أكثر انفتاحاً عن الحدود التي ينبغي رسمها للحكومة ورقابتها. نحتاج إلى مشرّعين مقتدرين في الإشراف، وتطوير ردود بعيدة النظر. كذلك نحتاج إلى محاكم منفتحة ومستقلّة تدعم القوانين ولا تصادق تلقائيّاً على ممارسات الوكالة، وتقارير دوريّة

عن أعمال الحكومة، وصحافة رأي عام نابضة، ومجموعات متابعة لتحليل أفعال الممسكين بالسلطة وفتح جدال معهم، إضافة إلى إطار تشريعي يستبق الأمور ويحذّر من المخاطر. وكذلك نحتاج جمهوراً مهتماً. وسوف أتحدث عن تلك الأمور في الفصل 13 أيضاً.

وهناك المستوى الثاني من الإشراف، وهو تكتيكي يلخّصه السؤال عن مدى الالتزام بالقوانين. وتتضمن آلياته الإجراءات والتدقيقات والموافقات وبروتوكولات التصدي للمشاكل وغيرها. مثلاً، درّبت «وكالة الأمن القومي» محلّليها على القوانين التي تتحكّم بعملها، ونُظُم التدقيقات التي مهمّتها التأكّد من الالتزام فعليّاً بالقوانين، كما أرست إجراءات في الإبلاغ وعقوبات تصحيحيّة في حال عدم الالتزام.

تمارس المنظّمات المختلفة إشرافاً تكتيكيّاً متبادلاً على بعضها بعضاً. وتعطي آلية الضمان مثلاً عن ذلك. من المؤكّد أننا نستطيع أن نثق بقوّات الشرطة عندما تنهض بعمليات التفتيش الواجبة عليها، ولكننا بدلاً من ذلك نطلب منها إبراز طلب التفتيش أمام طرف محايد- القاضي- الذي يضمن أنها اتّبعت القوانين قبل حصولها على أمرٍ من المحكمة بالتفتيش.

إن مفتاح الإشراف المتمكن هو الاستقلاليّة. ولذلك السبب، نبدي تشكّكاً دائماً بالتحقيقات الداخلية، حتى لو أجراها محامٍ متحمّس. كانت تلك القضية الرئيسة مع المسؤول الأول عن الخصوصيّة في «وزارة الأمن القومي». أتذكَر بوضوح ماري إلين كالاهان التي شغلت تلك الوظيفة بين عامي 2009 و2012. كانت مؤيّدة كبيرة للخصوصيّة، وأوصت بشطب برامج عدّة، بسبب مآخذ تتعلّق بالخصوصيّة. في المقابل، كانت تعمل تحت إدارة الوزيرة جانيت نابوليتانو، ما جعل عمل كالاهان مقتصراً على الاقتراحات. لو عملت كالاهان خارج الوزارة، لامتلكت صلاحيات

تشريعيّة أوسع. ينجز الإشراف التكتيكي بشكل أفضل على يد هيئات تقييم خارجيّة تتمتع بمعرفة واسعة وتملك ما يكفي من طواقم العمل.

يمكن التفكير بالفارق بين الإشراف التكتيكي والاستراتيجي باعتباره موازياً للفارق بين عمل الأشياء بطريقة صحيحة، والقيام بالشيء الصحيح. ونحن بحاجة لكلا الأمرين معاً.

لا يسير أيٌّ من الأمرين بفعاليّة من دون الموثوقيّة. من توكل إليهم السلطة ليسوا بمنأى عن إساءة استعمالها مع النجاة من العقاب؛ يجب أن توضع عقوبات لإساءة استخدام السلطة. يساوي الإشراف من دون موثوقيّة عدم تغيير أي شيء، وفق ما تعلّمنا التجربة مراراً وتكراراً. ووفق ما بينّ نسيم طالب، وهو مختصّ بتحليل المخاطر، يتدنى سوء استخدام المنظّمات لسلطاتها عندما يحسّ الناس أن مصيرهم معلّق بها(36).

تسهل المناداة بـ «الشفافيّة والإشراف والموثوقيّة»، لكن يصعب وضع هذه المبادئ موضع التطبيق فعليّاً. وعلى الرغم من ذلك، يجب أن نحاول، وسأبيّن في الفصل القادم كيف نفعل ذلك. تعطينا هذه الأشياء الثلاثة ثقة بالنفس تجعلنا نثق بالمؤسّسات القويّة. إذا كنا سنسلس القياد لهم، فيجب طمأنتنا بأنهم سيعملون لمصلحتنا، ولا يسيئون استخدام تلك السلطة.

التصميم المرِن

يعدُّ وضع تصميم للمرونة مبدأً أساسيّاً، بل شبه فلسفي، في هندسة النُظُم. غالباً ما يفترض بالحلول التكنولوجيّة أن تكون كاملة. لكن، كما نعرف جميعاً، الكمال أمر مستحيل، وفي صلب بنية الناس والمنظّمات والنُظُم أنها ليست تامة الكمال، بل فيها شيء من الخطل. وتعاني المنظّمات كلها وجود اختلالات فيها، بداية من الوكالات الحكوميّة وصولاً إلى الشركات المتعدّدة الجنسيّات.

لا تنجم الاختلالات من لاعبين سيئين داخل نُظُم من شأنها أن تكون كاملة لولاهم. تأتي الاختلالات من أشياء الدنيا العاديّة، والكادر المتوسط، والميل البيروقراطي. تعتبر ظاهرة «زحف المهمة»(*) أحد أشكال الاختلال.

يأتي شكل آخر للخلل من أشخاص داخل المنظّمات يركّزون على الحاجات الضيّقة للمنظّمة، بدل التفكير في الإملاءات الواسعة لأفعالهم.

وتأتي الاختلالات أيضاً من التغيير الاجتماعي على غرار التغيير في قيمنا مع مرور الزمن. ويضيف التقدّم التكنولوجي اهتزازات جديدة إلى تلك الموجودة في النظام، ما يخلّ بالاستقرار[37].

إذا كانت الاختلالات المنهجيّة أمراً لا مفر منه، فعلينا تقبّلها في القوانين والشركات والأفراد والمجتمع والمؤسّسات الحكوميّة[38]. يجب علينا تصميم نُظُم تتوقّع الاختلالات، وتستطيع العمل على الرغم من وجودها. إذا وجب فشل شيء ما أو خرابه، فالأفضل أن يحصل ذلك بطريقة متوقّعة. تلك هي المرونة[39].

في تصميم النُظُم، تتأتّى المرونة من اجتماع عناصر تشمل تحمّل الخطأ، والتخفيف، والتأقلم، والوفرة، والتعافي، والتمسك بالبقاء[40]. نحتاج تلك الأشياء في المشهديّة المعقّدة والمتغيّرة للتهديدات، وفق ما وصفته في الكتاب.

أُدافع عن ألوان متنوّعة من المرونة في نُظُمنا للرقابة ونُظُمنا التي تتحكّم في الرقابة أيضاً[41]. ويشمل ذلك المرونة حيال فشل البرامج والمُكوّنات الإلكترونيّة، والمرونة حيال الاكتشاف التكنولوجي، والمرونة حيال التغيير السياسي، والمرونة حيال الضغط والإكراه. أدافع عن تصميم للأمن يعطي المرونة حيال الأهواء السياسيّة المتغيّرة التي يحتمل أن تشرعِن الرقابة السياسيّة. يمنح تداخل السلطات وتعدّدها مرونة حيال الضغوط الإكراهيّة. تقدّم القوانين المتقنة الصياغة مرونة حيال القدرات التكنولوجيّة المتبدّلة. بديهي القول أيضاً إنه من المستحيل الوصول

(*) انظر الفصل السابع.

إلى المرونـة الكاملـة في تلك الأمور، ونافلاً القول باسـتحالة المرونـة الكاملة حيالها كلّهـا. عـلى الرغـم من ذلك، يجـب علينا بذل أفضل ما نسـتطيع، وصـولاً إلى نقطة افتراض الاختلالات في مرونتنا.

عالم واحد، وشبكة واحدة، وحلّ واحد

هناك نقاشـات كثـيرة في الولايات المتّحدة حول سـلطة «وكالة الأمن القومي»، وأنّ لجمهـا يعطـي قـوّة للآخريـن. إنّه نقـاش مغلوط. لسـنا أمام خيار بأن روسـيا والصـين وإسرائيل سـتتوقف عن التجسّـس، إذا توقّفت الوكالة عنـه. فعليّاً، يجب علينا حسم الخيار بشأن بناء بنية معلوماتيّة تحتيّة تكون هشّة أمام مهاجميها جميعاً، أو تكون مأمونة لمستخدميها كلهم.

منـذ تأسيسـها في 1952، محُضَـت «وكالة الأمـن القومي» الثقـة لتنفيذ مهمّات لهـا طبيعـة مزدوجـة[42]. في خطـوة أولى، انخرطـت «سـيغينت» في اعـتراض نُظُم الاتّصالات لدى أعداء أميركا. وبعدها، تولّى قسـم «أمن الاتّصالات»، «كومسك» (COMSEC)، حماية الاتّصالات العسـكريّة الأميركيّة وبعض الاتّصالات الحكوميّة مـن احتـمال اعتراضها من قِبَل أعـداء. وبدا منطقيّاً الجمع بـين المهمّتين؛ لأن معرفة آليات التنصّت ضروريّة للحماية من التنصّت.

كانـت المهمّتـان متكاملتـين؛ لأن البلـدان المختلفـة اسـتخدمت نُظُـماً مختلفة في الاتّصـالات، وكذلك اسـتخدم المدنيّون والطواقـم البشرية العسـكريّة نُظُماً مختلفة أيضـاً. ووفـق ما وصفته في الفصـل 5، لم يعد ذلك العالم موجـوداً. وحاضراً، باتت مهمّتا «وكالة الأمن القومي» متضاربتين.

ربـما يحدّد القانـون الطُـرُق المشروعة للرقابة، لكـن التكنولوجيا هـي التي تقرّر مـدى الرقابـة وإمكاناتها. عندما نقـرّر تقنيّات الاتّصالات التي يجـب أن نتبنّاها، لا نستطيع أن ننظر إلى بلدنا [الولايات المتّحدة] وحده. يجب أن ننظر إلى العالم بأسره.

لا نستطيع أن نوهـن شـبكات الأعداء، وإبقاء شـبكاتنا محميّـة وآمنة في الوقت نفسـه. وإذ تسـتغل أجهزة الاسـتخبارات عالميّاً الثغرات في النُظُـم الإلكترونيّة كي تتجسّـس على بعضها بعضاً، تسـتخدم عصابات الإجرام الثغرات نفسها كي تسطو عـلى كلـات المرور التـي تسـتعملها في حسـاباتك المصرفيّـة؛ لأننا نسـتعمل جميعنا المنتجـات والتقنيّـات والبروتوكولات والمعايـير ذاتها؛ يكون لزامـاً علينا الخيار بين إعطاء كل شـخص القدرة للتجسّـس على الآخر أو نجعل التجسّس أمراً صعباً على الجميـع. إنهـا الحريّـة في مواجهة التسـلّط، فإما أن ننجـو جميعاً أو نهـوي كلّنا. كتب البروفسـور جاك غولد سـميث، وهو أسـتاذ قانون في جامعة هارفرد شغل منصب المدّعـي العـام أثنـاء حكـم الرئيس جـورج دبليو بـوش: «كل سـلاح هجومي هو (احتمالاً) جزء من نظامنا الدفاعي، والعكس بالعكس»[43].

ومثـلاً، يفـرض «قانـون مسـاعدة الاتّصـالات في تطبيـق القوانين» أن تسـمح الـدارات الإلكترونيّـة في الهواتف، بتنصّت [حكومي] على المكالمات. ربما نتسـامح مع ذلك بالنسـبة لقوى الشرطـة الأميركيّة؛ لأننا نثق عمومـاً بالإجراءات القضائيّة اللازمـة للسـماح للشرطـة بالتنصّـت، ونميـل للافـتراض بـأن الشرطـة لـن تسيء اسـتخدام صلاحياتهـا. في المقابـل، تُباع تلـك الدارات نفسـها عالميّـاً- أذكر بقصة التجسّـس على خلوي في اليونان، التـي وردت في الفصل 11 -مع امتلاكها للقدرة عـلى إتاحة التنصّت. إذاً، يعود الخيـار لنا: إما أن يكون الكل قادراً على التنصّت، أو ألا يفعل أحد ذلك.

نطبق الوصف نفسـه على الأداة الإلكترونيّة المسـّماة «آي أم أس آي- كاتشر»(*) التـي تتولى اعتراض المكالمـات الخلوية والـ «ميتا- داتا» المتّصلـة بها. ربما كانت أداة «سـتنغراي» الشـبيهة بــ «آي أم أس آي- كاتـشر» سـلاحاً سريّـاً لـدى الـ «إف بي آي»، لكنهـا تقنيـة لم تعد سريّة أبـداً[44]. هناك عشرات من تلك الأدوات منشـورة

(*) هي أساساً برج مزيّف للاتصالات الخلوية. راجع الفصل 5

حـول العاصمة واشـنطن، لكن بقية البلاد تدار من قِبَل مـا لا يُعلم من المنظّمات أو الوكالات الحكوميّة[45]. وباطّراد، تدنو لحظة استخدامها إجراميّاً. ولأننا عملنا على أن تكون شـبكات الاتّصـالات الهاتفيّة قابلة للاختراق من قِبَـل تلك الأدوات كي تسـاعد التحقيقات في الجرائم، فإنّنا أتحنا بالضرورة أن تستخدم ضدّنا من المجرمين والحكومات الأجنبيّة.

في الفصـل 11، أعطيت أمثلـة جمّة عن ذلك الأمر. وعموماً، يجب علينا أن نقرّر بشـأن البنيّة التحتيّة للاتّصالات التي نصبو إلى إنشـائها: هل تكون مكرّسـة للأمن والرقابة والخصوصيّة والمرونة أو لا؟ وعندها يسـتطيع *كل* شـخص استخدام تلك البنية التحتيّة.

13

حلول للحكومة

في سياق كشوفات سنودن عن رقابة «وكالة الأمن القومي»، تبيّن أن الاقتراحات بشأن طُرُق إصلاح الاستخبارات القوميّة كانت غزيرة. في العام 2013، ألّف الرئيس باراك أوباما لجنة للمراجعة بشأن الرقابة والاستخبارات القوميّة، وتوصّلت تلك اللجنة إلى 46 توصية بصدد «وكالة الأمن القومي»[1]. في العام 2014، وقّعت 500 منظّمة وخبير ومسؤول من أرجاء العالم كافة، كنتُ واحداً منهم، وثيقة «مبادئ دوليّة عن تطبيق حقوق الإنسان في رقابة الاتّصالات» (International Principles on the Application of Human Rights on Communications Surveillance) التي يُشار إليها غالباً باسم «المبادئ الضروري والنسبية» (Necessary & Proportionate Principles)[2]. وناقش الكونغرس وثائق عدّة تتضمّن إصلاحات صغيرة، ربما أقرّ بعضها عند ظهور الكتاب.

في هذا الفصل، أناقش الأمن القومي وإنفاذ القانون، وأقدّم توصيّات عامة، بأكثر من كونها توصيفات تشريعيّة دقيقة، عن السياسة التي يجب اتّباعها في الأمرين كليهما. من السهل تنفيذ بعض التوصيات، لكن الأخرى تقترب من كونها أمنيّات. وتعبّر كلها عن الطريق الذي أعتقد بأنّه يجب على الحكومة سلوكه.

لا أحاجج لمصلحة حرمان الحكومة كليّاً من الرقابة أو التجسّس. نحن فعليّاً منحنا صنّاع السياسة منذ زمن، ما يكفي من القوى لغزو خصوصيّة المواطن

والنفاذ إلى بياناتهم ومعلوماتهم. فعلنا ذلك عن معرفة مسبقة- وبإرادة منا أيضاً- لأن ذلك يساعد في كشف الجرائم، ما من شأنه أن يجعلنا أكثر أماناً. يكمن الهدف فعليّاً في التوصل إلى توازن بين حيازة المؤسّسات الحكوميّة تلك القوى من جهة، وضمان عدم إساءة استخدامها من الجهة الأخرى. إذ نحتاج إلى الأمن الذي تؤمّنه الحكومة، كما نحتاج إلى أن نكون آمنين من الحكومة نفسها. وتحاول التوصّل إلى ذلك التوازن، وثائق كـ «دستور الولايات المتّحدة» و«شرعة الاتحاد الأوروبي»، وإجراءات كالحصول على إذن قضائي للتفتيش. واختل ذلك التوازن في سياق سعينا المجنون إلى الأمن ضد الإرهابيّين عقب هجمات 9/ 11.

"مبادئ عالميّة عن تطبيق حقوق الإنسان في رقابة الاتّصالات- ملخّص 2014"[3]

شرعيّة: يجب صوغ حدود الحق في الخصوصيّة بوضوح ودقّة في القوانين، ويجب مراجعتها بانتظام للتثبّت من التناسب بين حمايات الخصوصيّة وسرعة التغيّرات التكنولوجيّة.

هدف قانوني: يجب ألا يسمح بالرقابة على الاتّصالات سوى في سياق السعي إلى تحقيق الأهداف المهمّة للدولة.

ضرورة: يقع على الدولة واجب إثبات أن نشاطاتها في رقابة الاتّصالات ضروريّة لتحقيق هدف قانوني.

ملائمة: يجب أن تكون آلية رقابة الاتّصالات فعّالة في تحقيق هدفها القانوني.

تناسب: يجب أن ينظر إلى رقابة الاتّصالات كعمل تدخّلي من أعلى مستوى، ويتدخّل في حقوق الخصوصيّة وحرية الرأي والتعبير، إضافة لكونه يهدد أسس المجتمع الديمقراطي. وعلى نحو نموذجي، تتطلّب الرقابة المناسبة في الاتّصالات تخويلاً مسبقاً من مُكوّن في السلطة التشريعيّة.

مُكوّن السـلطة التشريعيّة: التحديد بشـأن رقابة الاتّصـالات يجب أن يكون من قِبَل مُكوّن في السلطة التشريعيّة يتمتع بالاستقلاليّة وعدم الانحياز.

إجراء مناسب: يتطلّب الإجراء المناسب إخضاع التدخل في حقوق الإنسان إلى إجراءات قانونيّة تكون متاحة للعموم، وأن تطبق بسواسيّة ضمن لجنة استماع عادلة وعلنيّة.

تنبيه المسـتخدم: يجب تنبيه الأفراد بشـأن قرار فرض رقابة على اتّصالاتهم. في ما عـدا حالاً وجد فيها مُكوّن السـلطة التشريعيّة أن التنبيه يـؤذي التحقيق، ويجب أن يعطى الأفراد فرصة لتحدي فرض الرقابة قبل حدوثها.

الشـفافيّة: يقـع على الحكومـة واجب إتاحة معلومـات كافية وعلنيّـة، ما يمكن الجمهـور العـام من فهـم طبيعـة نشـاطاتها الرقابيّة وأمديتهـا. وعمومـاً، يجب على الحكومـة عـدم منع مقدّمي الخدمات من نشر تفاصيل عـن طبيعة ومدى تعاملاتهم الخاصة مع الحكومة في ما يتّصل بالرقابة.

إشراف الجمهـور: يجـب عـلى الحكومـات إرسـاء آليات مسـتقلّة لـلإشراف بما يضمـن شـفافيّة رقابـة الاتّصـالات وموثوقيّتها. يجـب أن تمتلك آليـات الإشراف سـلطة الوصول إلى المعلومات كافة التي يحتمل أن تكون ذات دلالة بالنسبة لأفعال الحكومة.

نزاهـة الاتّصـالات والنُظُم: يجب ألا يُرغـم مقدمو الخدمـات والشركات البائعة للبرامج والمكوّنات الصلبة، على وضع قدرات رقابيّة أو «أبواب خلفيّة» في نُظُمِهم؛ أو جمع أو الاحتفاظ بمعلومات معيّنة لمجرد خدمة أهداف رقابة الدولة.

ضوابـط التعـاون الـدولي: وفقـاً للحـال، ربـما تسـعى الحكومـات إلى الحصول على مسـاعدة مـن مقدّم خدمـة أجنبي، بهدف ممارسـة رقابة. يجـب أن يضبط ذلك باتفاقيّـات واضحة وعلنيّة تضمن تطبيق أعلى مسـتوى في حماية الخصوصيّة، يكون قابلاً للاعتماد عليه في الأحوال كلها.

ضوابط ضد الوصول غير المشروع: يجب فرض جزاءات مدنيّة وجرميّة على كل طرف تثبت مسؤوليته عن ممارسة رقابة إلكترونيّة غير شرعيّة؛ ومن تطالهم تلك الرقابة لهم الحق في الوصول إلى آليات قانونيّة تضمن تعويضهم بشكل فعّال. كذلك يجب تقديم حماية قويّة لمطلقي صافرات الإنذار الذين يكشفون نشاطات رقابيّة مهدّدة لحقوق الإنسان.

أنا أتحدّث أساساً عن الولايات المتّحدة، على الرغم من أن التوصيات الواردة في هذا الفصل تصلح في أمكنة أخرى. في الولايات المتّحدة، يستطيع الرئيس تنفيذ بعض تلك التوصيّات استناداً إلى السلطة التنفيذيّة بشكل أحادي، وبعضها يتطلّب موافقة الكونغرس، لكن بعضاً آخر يحتاج إلى سنّ تشريعات جديدة. وتملك بلدان أخرى قوانين خاصة بها عن الفصل بين السلطات. وبالطبع، ثمة بلدان يتطلّب فيها تنفيذ تلك التوصيات إحداث تغيير جذري في الحكومة.

سريّة أقل، شفافيّة أكثر

منذ 9/ 11، زعمت إدارتا بوش وأوباما تكراراً أن مستويات السريّة العالية أمر ضروري لمنع العدو من معرفة ما نفعله[4]. هناك مستويات من السريّة مورست في الحرب العالميّة الأولى، وما زال بعض منطقها صالحاً. تملك الحقائق التكتيكيّة قيمة كبرى لمدّة معيّنة، ومن المهم الاحتفاظ بها سراً طيلة تلك المدّة. وأحياناً، تبرز الحاجة للاحتفاظ بأسرار كبرى: كالمفاوضات مع البلدان الأخرى، هويّات العملاء الأجانب، الخطط العسكريّة وبعض مناحي الاستخبارات القوميّة[5]. وفي عودة إلى الفارق المهم بين التجسّس والرقابة، تتطلّب نظمنا في التجسّس سريّة أعلى كثيراً مما تفعله نظيرتها في الرقابة.

في المقابل، نستطيع أن نكون أكثر شفافيّة في نواح عدّة. قارن السريّة الكثيفة التي تحيط بعمل «وكالة الأمن القومي» مع نطاق مُشابِه نحرز فيه نجاحات بصورة روتينيّة من دون رقابة مكثّفة: الشرطة ومكافحة الجريمة. ينظّم التعديل الرابع في

الدستور الأميركي قدرة الشرطة على ممارسة الرقابة، كما أن الأحكام القضائيّة بشأنها علنيّة. يستطيع المجرمون قراءة تلك الأشياء كلها، أو استئجار محام متضلّع فيها، ثم صنع دليل تفصيلي عن كيفيّة الاستفادة بدقة من الثغرات في القانون[6]. هناك الكثير من الثغرات، ويجيد كثيرون من محامي الدفاع العثور على طريقهم بواسطتها. وعلى رغم ذلك، لا يتوقف عمل الشرطة، وينجح باستمرار في إلقاء القبض على المجرمين وإدانتهم[7].

وبصورة أعم، فإن معظم ما يتعلق بالشرطة ومكافحة الجريمة معلن للعموم. نعرف ميزانيات قوى الشرطة في البلاد كلها. نعرف قدراتها. نعلم مدى فعاليّتها. نعرف ما تفعله ومدى كفاءتها في ذلك. لا نعرف هويّة ضباط الشرطة السريّين، لكننا نعرف عموماً كيف يُستَخدَمون، وما يستطيعون الإقدام عليه، وما لا يستطيعون. كل تلك الأمور معلنة، ويعرفها جيّداً أولئك الذين يعطون الشرطة سلطة على الناس، مثلما يعرفها من يخطط لارتكاب جرائم. وعلى الرغم من ذلك، تستطيع الشرطة دوماً التصدي للجرائم.

يبرهن ذلك على أن المستوى الحالي من السريّة في العمل ضد الإرهاب مبالغ به. إذ يطبّق مستوى عسكري من السريّة على ما عُدّ دوماً شأناً محليّاً. لا يفوق الإرهابيّون المجرمين ذكاءً. ولا يوقع الإرهابيّون قتلى وخراباً أكثر مما يفعل المجرمون، ويتلخّص الأمر في أننّا نخشى الإرهاب أكثر[8]. يلزمنا نقل مبادئ الشفافيّة من القوى التقليديّة لإنفاذ القانون إلى الأمن القومي، بدلاً من زيادة السريّة حول قوى إنفاذ القانون، على نحو ما شرعنا به فعليّاً بكل أسف. يجب أن نصنع نُظُماً رقميّة تبقي علينا آمنين، حتى عندما تكون تفاصيلها علنيّة ومعروفة من العدو[9]. بات حفظ الأسرار أشد صعوبة اليوم، ونكون في وضع أفضل إذا قلّلنا الأسرار عدداً.

في ثمانينيات القرن العشرين، أوقفت الولايات المتّحدة مساعيها لجعل بحوث التشفير سريّة؛ لأن نتيجة تلك المساعي كانت الإساءة إلى مهندسينا وعلمائنا في

الرياضيـات، بالمقارنـة مـع أقرانهم في بلدان أخـرى[10]. وفي وقـت قريب، أوقفت الولايات المتّحدة مسـاعيها لجعل بحوث تصنيع الفيروسات البيولوجيّة سريّة؛ لأن أحداً ما سينشر تلك المعلومات بغض النظر عما نفعله. ويدرك المفكّرون العسكريّون حـاضراً أنّ كثـيراً مـن الأسرار العسـكريّة الاسـتراتيجيّة يصعـب حفظها؛ بسـبب القدرات الشاملة للتصوير بالأقمار الاصطناعيّة وما يشبهها من التقنيّات[11]. يجدر التفكير بشأن السريّة الحكوميّة في ما يتّصل بالرقابة، بطرق مُشابهة لما ورد أعلاه.

توجد قوانين لشفافيّة الرقابة في الولايات المتّحدة. في نصه الأصلي للعام 1968، تطلّـب قانـون التنصّت عـلى خطوط الهاتف أن تقـدّم الحكومة تقاريـر علنيّة مكثّفة عن اسـتخدامها للتنصّت. وتضمّنت تقارير بحجم 200 ورقة سـنويّاً عن التنصّت الهاتفـي كميّـات ضخمة مـن التفاصيل. أتاح ذلـك للناس التثبّت ممـا يفعله مكتب الـ «إف بي آي»، والتأكّد من عدم إسـاءته لسـلطاته. ظهرت المشـكلة مع التوسّـع في الأشـكال الأخـرى من الرقابة بعـد 9/ 11، مع عدم تطلّب تقاريـر مماثلة. يجب إصلاح ذلك الخلل.

يجـب عـلى الحكومة الأميركيّة نشر توصيف تفصيلي غـير سريّ عن أمدية تجميع المعلومات الاسـتخباراتيّة ودرجة اتسـاعها. وكذلك نشر تبريـرات قانونيّة لبرامجها في الاسـتخبارات. ويجب أن تنشر معلومات عن نوع البيانات التي تجمعها سلطاتها المختلفـة وكميتها، إضافـة إلى معلومات عن عمليات التقليـص وقوانين الاحتفاظ بالبيانـات. كـما يجـب عليها نـشر الآراء العامة لمحكمة «فيسـا»(*) التـي تشرف على نشاطات الرقابة لـ «وكالة الأمن القومي» بموجب قانون «فيسا» وتعديلاته. يفرض القانون الإبقاء على أسـماء الناس والمنظّمات الخاضعة للترصّد، لكنه لا يفرض ذلك بالنسبة للتشريعات التي تعمل تحتها منظّمات الرقابة.

(*) انظر الفصل الخامس.

إشراف أكثر وأفضل

للسيطرة على رقابة «وكالة الأمن القومي»، نحتاج إلى تحسين وزيادة الإشراف على الاستخبارات القوميّة وقوى إنفاذ القانون معاً.

يأتي الإشراف الاستراتيجي أولاً. إذ بررّت «وكالة الأمن القومي» أفعالها دوماً بالإشارة إلى إشراف الكونغرس عليها[12]. وزعم قادتها أن موظّفي الوكالة بالكاد انصاعوا للقوانين التي صاغها الكونغرس أو الأوامر التي وقّعها الرئيس. ووفقاً لأحد بياناتها الصحافيّة الرسميّة، «تمارس «وكالة الأمن القومي» نشاطاتها كافة بالتوافق مع ما هو مطبّق من القوانين والتوجيهات والسياسات». ليس ذلك صحيحاً البتّة، بل يحمل خداعاً عميقاً. ونعرف من وثائق أُسقِطت سريّتها أخيراً عن آراء «محكمة فيسا»، خصوصاً تلك التي كتبها القاضي جون بايتس، أن «وكالة الأمن القومي» قدّمت تشخيصات خاطئة إلى المحكمة، ولم تنصع لمتطلّبات التقليص [في مدى نشاطاتها المُجازة] وتجاوزت تكراراً تفويضاتها القانونيّة[13].

تلاعبت «وكالة الأمن القومي» بالقوانين التي تضبط إشراف الكونغرس عليها؛ كي تضمن عدم حدوث تفهّم حقيقي أو مراجعة حاسمة[14]. وتكوّنت الوثائق التي قدّمتها الوكالة للكونغرس إما من نصوص دعائيّة مُصمّمة بهدف الإقناع، أو وثائق مملوءة باللغة التقنيّة بهدف إحداث التباس. كما لا يتمكن أعضاء الكونغرس من تحريك تلك الوثائق من الغرف المؤمّنة التي تخزّن فيها، ولا يستطيعون إزالة الملاحظات التي يكتبونها[15]. جلّ ما يستطيعه أعضاء الكونغرس هو استقدام موظّفين مأذون لهم أمنيّاً؛ كي يشرحوا لهم معنى تلك النصوص ودلالتها، مع ملاحظة أنّ قلّة من صُنّاع التشريع لديهم موظفون يحوزون أُذونات أمنيّة متقدّمة المستوى ولديهم خبرة ملائمة[16]. ويضاف إلى ذلك أن الوكالة مارست ضغوطاً كثيفة عليهم[17]. إذ صرّح السيناتور رون وايدن أن المسؤولين الكبار في الاستخبارات قدّموا «تصريحات مضلّلة أو مخادعة» في لجان الاستماع في

الكونغرس. وكذلك استنتجت السيناتورة ديانا فاينشتاين، رئيسة «اللجنة المختارة من مجلس الشيوخ عن الاستخبارات»، أن لجنتها وبكل أسف «لم تكن تُخبَر بطريقة مناسبة»[18] من مجتمع الاستخبارات عن نشاطاته، على الرغم من الانحياز المديد لفاينشتاين لمصلحة الرقابة الحكوميّة. وسمّى آلان غرايسون، عضو الكونغرس عن فلوريدا، إشراف الكونغرس على «وكالة الأمن القومي» بأنّها «نكتة»[19].

في العام 2014، دعاني 6 أعضاء في الكونغرس من الحزبين الجمهوري والديمقراطي لعرض خلاصة عن نشاطات الوكالة[20]. ولأنني راجعت مجموعة كبيرة من وثائق سنودن غير المنشورة، كنت أعرف عن نشاطات الوكالة أكثر منهم. كيف يمكن لديمقراطيتنا أن تستمر إذا كانت أفضل المعلومات التي يستطيع الكونغرس معرفتها، آتية مني؟

من ناحية أخرى، لا يرغب بعض المُشرّعين ممارسة مهمة الإشراف المناطة بالكونغرس. يرجع بعض التلكؤ إلى الرغبة في الإنكار السعيد. ويكون الأمر أكثر أماناً في السياسة، عندما يترك للسلطة التنفيذيّة مهمة صنع القرارات، إذا فلتنصب سيول الحرارة على تلك السلطة عند حصول أمر سيئ. وثمّة مغامرة سياسيّاً في الوقوف بوجه قوى إنفاذ القانون[21]. وبالنتيجة، لم تغامر سوى قلّة من أعضاء لجنة فاينشتاين بالذهاب إلى الغرف الأمنيّة في «وكالة الأمن القومي».

تفسّر الوكالة سلطاتها بشراسة كأنها تصارع من أجل النجاة بنفسها. في الفصل 5، ناقشت ثلاث سلطات مختلفة تستخدمها الوكالة لتبرير نشاطاتها في الرقابة: الأمر التنفيذي رقم 12333، والبند 215 من «قانون باتريوت» والبند 702 من «قانون تشريعات فيسا».

يتميّز الأمر التنفيذي 12333، وهو وثيقة رئاسيّة للعام 1981 يأذن للوكالة بمعظم نشاطاتها الرقابيّة، بأنه متسامح معها إلى حدّ لا يصدّق[22]. ويُفترض أنه يسمح للوكالة بممارسة الرقابة خارج الولايات المتّحدة، لكنه يعطي الوكالة أيضاً

سلطة واسعة لجمع بيانات عن أميركيّين[23]. ولا يقدّم سوى حماية قانونيّة واهية للبيانات التي تُجمع عن أميركيّين خارج بلادهم، وأقل منها كثيراً بالنسبة للبيانات التي تجمع مصادفة عن مئات ملايين الأميركيّين. ولأنه توجيه رئاسي وليس قانوناً، لا تملك المحاكم سلطة حياله، كما لا يمارس الكونغرس سوى الحدّ الأدنى من الإشراف عليه. يضاف إلى ذلك، على الأقل في 2007، اعتقد الرئيس أنّه يستطيع تعديله أو تجاهله، سراً ووفقاً لإرادته[24]. وبالنتيجة، لا نعرف سوى القليل جداً عن كيفيّة تفسير الأمر التنفيذي 12333 من قِبَل «وكالة الأمن القومي».

لم يقصد بالبند 215 من «قانون باتريوت» أن يكون تفويضاً برقابة عامة، ومن الممكن إعطاء حجج قويّة للقول إن لغته لا تجيزها. إذ كانت الفكرة هي تمكين الـ «إف بي آي» من الحصول على معلومات «لها دلالتها بالنسبة لتحقيق [من الأمن القومي] يكون مرخصا به قانونيّاً»- بمعنى أنه تحقيق له موضوع محدّد- يحصل على معلوماته من مصادر واسعة، لم يكن بوسعه الوصول إليها قبل ذلك. وضربت الرئاسة مثلاً بمعلومات عن كُتبٍ حصل عليها شخص مشتبه فيه من مكتبة، ربما قرأ «المرشد العملي للفوضوي» أو ما يشبهه[25]. في الواقع، أثناء نقاش مشروع ذلك القانون، كان يشار إليه باسم «الشرط بصدد المكتبة». واقتصر شأنه على تمكين مكتب الـ «إف بي آي» من طلب معلومات كان بمكنته الحصول عليها بواسطة مذكرة قضائيّة من محكمة كبرى- مع الاقتصار على «البيانات الوصفيّة»، وليس المحتوى- فأتاح للـ «إف بي آي» الحصول على المعلومات عينها من دون انعقاد محكمة. بدا ذلك منطقيّاً؛ لأنه لا توجد فعلياً محكمة كبرى بشأن تحقيقات الأمن القومي.

أيّاً كان الأمر، فعندما أقرّ «قانون باتريوت» في 2001، غربل محامو الأمن القومي في وزارة العدل القانون بحثاً عن ثغرات فيه. وعلى الرغم من أن القانون قصد تسهيل المراقبة الموجّهة، قرّر أولئك المحامون أنّه بالمستطاع توسيع حدوده ليكون تخويلاً بالرقابة العامة. وعلى الرغم من أنّه أعطى تمكيناً للـ «إف بي آي»

وحـده، فإنّهم قرّروا أنّ ذلك المكتب يسـتطيع أن يطلب نقـل المعلومات إلى «وكالة الأمـن القومـي». في البدايـة، فعلوا ذلك من دون موافقـة أي محكمة على الإطلاق. وبالنتيجة، قرّروا أن تنظر مسـائلهم أمام «محكمة فيسـا» السريّة[26]. وفي غياب من يقـدّم رأيـاً معارضاً، كانـوا قادرين على إقناع القاضي بأن *كل ما يفعلونه* له «دلالة» بالنسـبة لتحقيـق ما. كان ذلك تفسـيراً جديـداً لمعنى كلمة «دلالة»، وهو تفسـير لا يسـتطيع اجتياز أبسـط تدقيق. إذا كانـت كلمة «دلالة» ليـس بمقدورها أن تفرض حدوداً على تجميع المعلومات لأن كل شيء له دلالة، فلماذا أصلاً وُضِع ذلك التقييد في القانـون؟ حتـى عضـو الكونغرس جيم سنسـنبرينر الـذي تولى صياغـة «قانون باتريـوت»، تولّتـه الدهشـة عندما علم أن الوكالة اسـتخدمت ذلـك القانون لتبرير جمع معلومات بفرضها رقابة عامة على الأميركيّين[27]. ووصف ذلك بقوله: «يشبه الأمر اغتراف المحيط لضمان التقاط سمكة»[28].

البنـد 702 مـن «قانـون تشريعات فيسـا» لـه قصة مختلفـة قليلاً. إذ افـتُرِضَ أن ذلك التشريع يقدر على حلّ مسـألة محدّدة. يلجأ مسـؤولو الإدارة الرئاسيّة إلى رسم الإشـكال التالي: يتحدّث إرهابي من السعودية مع إرهابي في كوبا، والبيانات تتدفق عـبر الولايات المتّحدة لكن يُفترَض بـ «وكالة الأمن القومي» ألا تتنصّت إلا خارج بلادهـا. ويحاجج المسـؤولون بـأنّ ذلك يمثّـل أمراً غـير فعّال، وسـمح البند 702 للوكالة بأن تلتقط مكالمات من خطوط تمرّ في الولايات المتّحدة.

مـرّة أخـرى، لا شـيء في البند 702 يخـوّل فرض رقابة عامة. وتـبرّر الوكالة اسـتخدامه بإساءة اسـتعمال كلمة «عرضي». إذ يجري اعتراض كل شيء، «البيانات الوصفيّـة» والمحتـوى معـاً، ويفتـش أوتوماتيكيّاً بهـدف العثور على عنـاصر مهمّة للوكالـة. تزعـم الوكالـة أن الأشـياء التي تسـعى إلى تخزينهـا تملك أهليـة اعتبارها بحثـاً. وتصنّف الأشـياء الأخرى كلهـا بوصفها «عرضيّة»، وطالما أن «الشـخص-الهـدف» المطلوب هو خـارج الولايات المتّحدة، فلا بأس في ذلك. هناك تشـبيه مجدٍ لتلك الصورة يتمثّل في السـماح لضباط الشرطة بتفتيش بيوت المدينة كلها بحثاً عن

شخص يعيش طبيعيّاً في بلغاريا. في تلك الحال، يحتفظ الضبّاط بما يصادفونه عرضاً من أدلة عن أي جريمة، ثم يحاججون بأن عمليات التفتيش الأخرى يجب أن لا يتم احتسابها تفتيشاً لأنها لم تعثر على شيء، وأن ما عثروا عليه يجب قبوله كدليل لأنه التُقِط «عرضيّاً» أثناء البحث عن البلغاري. يمنع التعديل الرابع في الدستور الأميركي ذلك النوع تحديداً، ويصنّفه كـ «غير منطقي»، ولأسباب وجيهة تماماً.

أظن أنّه عندما ظهر «قانون تشريعات فيسا» في 2008، كانت «وكالة الأمن القومي» على وعي تام بما تفعله، لذا عمدت إلى إعمال مطرقتها بكلمات ذلك القانون كي تفسح المجال أمام تفسيرها الخاص له. ولربما قدّمت قيادتها خلاصات للجان الاستخبارات في مجلسي النواب والشيوخ، عن قراءتها لنصوصه. ومن المؤكّد أنها لم تخبر جميع أعضاء المجلسين، وكذلك الشعب الأميركي. أعتقد أن كثيراً من تلك الأفعال سوف يتبيّن مخالفتها للدستور. إذ يحمي التعديل الرابع في الدستور الأميركي من عمليات التفتيش غير المنطقية، ومن المصادرات غير المنطقيّة أيضاً. ويعدُّ مجرد الحصول على نسخة من الكتلة الرئيسة لبيانات شركات كـ «فريزون» (Verizon)، مصادرة غير قانونيّة أيضاً.

تتمثّل المشكلة في أن السلطات التشريعية والتنفيذية والقضائيّة تخلّت عن سلطاتها في الإشراف. في المسار الديمقراطي الطبيعي، يجري تحويل قانون ما إلى قواعد تتحوّل بدورها إلى إجراءات عمليّة؛ ما يجعل كل خطوة عرضة للتفسيرات، وهو أمر يفرض وجود إشراف مستمر بواسطة تلك الخطوات كلها. من دون ذلك الإشراف، يحتمل أن تسيء الوكالات الحكوميّة استخدام سلطاتها. حدث ذلك في سبعينيات القرن الماضي، عندما تجسّست «وكالة الأمن القومي» والـ«إف بي آي» على الأميركيّين ضمن مشروعين سُمّيا «شامروك» (SHAMROCK) و«مينارت» (MINARET)، إضافة إلى مشروع لم تجر تسميته وكان جزءاً من الحرب على المخدرات. ويتكرّر ذلك حاضراً[29].

ليس الأمر ظاهرة أميركيّة حصرياً. حدث الأمر عينه في المملكة المتّحدة عام 2000، عند تبني «قانون تنظيم سلطات التحقيق»[30]. إذ استخدمت «القيادة الحكوميّة للاتّصالات»، وهي النظير البريطاني لـ «وكالة الأمن القومي»، البند 16 (3) الذي جرى إغفاله إلى حد كبير عند نقاش القانون، كي تتجسّس على مواطنين بريطانيّين. وعملياً، استُبعِد البند من النقاش، بل استشرس بعض البرلمانيّين دفاعاً عن صياغته الغامضة والملتوية عمداً[31]، التي لم تكن عملياً تجيز الرقابة العامة، ولم يحل ذلك دون الوصول إلى استخدام ذلك البند مبرّراً للرقابة العامة[32]. وشخصيّاً، أعتقد أن فكرة البند 702 في «قانون تشريعات فيسا» جاءت من البند 16 (3) في «قانون تنظيم سلطات التحقيق».

في العام 2013، حاول الرئيس أوباما طمأنة الأميركيّين بأن برامج الرقابة في «وكالة الأمن القومي» تخضع للمراجعة، وتتطلّب موافقة الأذرع الثلاث للحكم[33]. لم يكن خطابه سوى تضليل[34]. قبل كشوفات سنودن، لم تعرف بالمدى الكامل لنشاطات الرقابة الحكوميّة سوى قلّة من أعضاء السلطة التنفيذيّة، وكُشِفَت جزئيّاً لبعض الأعضاء الرفيعي المستوى في السلطة التشريعيّة، ولم تُجز تشريعياً إلا من قبل محكمة «فيسا» التي رفضت 11 من أصل 34 ألف طلب للتفويض تقدّمت بها «وكالة الأمن القومي»، في الفترة الممتدة بين تأسيس «فيسا» في 1979 والعام 2013. لا يعّبر ذلك عن إشراف فعلي. وإنصافاً، يظل ذلك إشرافاً أكبر مما يحدث في بلدان كثيرة، بما فيها بلدان ديمقراطيّة كفرنسا وألمانيا وبريطانيا.

يحاول بعض أعضاء الكونغرس فرض قيود على الوكالة، ويمكن لبعض مقترحاتهم أن يكون مؤثّراً، بل يصنع فارقاً في عمل الوكالة. وعلى الرغم من ذلك، لا يحدوني الأمل بأن يقوم الكونغرس حاضراً بإصلاح مُجْدٍ؛ لأن كل المقترحات المتعلّقة بالوكالة تركّز على برامج وسلطات محدّدة. إذ تتناول تلك المقترحات مثلاً برنامج الوكالة لجمع «البيانات الوصفيّة» تحت البند 215 [35]، والتجميع الواسع للتسجيلات تحت البند 702 وهكذا دواليك[36]. لا تستطيع تلك المقاربة المجزّأة

أن تكـون فعّالـة. لقد تجاوزنـا مرحلة أن يسـتطيع تدخّل تشريعي بسـيط أن يُحدِثَ فارقـاً. وحـاضراً، هنـاك كثير مـن السريّة في عمـل الوكالة، كما تتناقـل مجموعة من برامجها تبريرات قانونيّة متنوّعة[37]. عندما ترفض الشركات رسائل الوكالة، ترميها الحكومـة بأمـر يسـتند إلى البنـد 215[38]. وتكراراً، هـدّدت الوكالة بأنـه إذا قلّص الكونغـرس صلاحيتهـا المسـتندة إلى البنديـن 215 و207، فسـوف تنقـل البرامج المُقلّصة إلى صلاحية الأمر التنفيذي رقم 12333 المتسّم بتسامح أكبر معها، إضافة إلى كونه أقل سيطرة ويتمتع بسريّة كبيرة[39].

ثمـة محـاولات أخرى لـلإشراف. في العام 2013، شـكّل الرئيـس أوباما لجنة مراجعـة لـ «وكالـة الأمن القومـي»، حازت سـلطات كبيرة في النفاذ إلى نشـاطات الوكالـة وقدراتهـا. وأنتجـت اللجنة تقريراً ممتازاً تضمّن 46 توصية بشـأن سياسـة الوكالة[40]، كما وافق الرئيس أوباما على تنفيذ مجموعة كبيرة منها[41]. يبقى السؤال عـما أنجـزه الرئيس فعليّاً. في العام 2004، أنشـأ الكونغرس «هيئة الإشراف بصدد الخصوصيّـة والحريّـات المدنيّـة» بتوصيـة مـن «لجنـة التحقيـق في 9/ 11»، بهـدف الإشراف على قضايا الأمن القومي[42]. افتقرت اللجنة إلى عدد كافٍ من الموظفين، كـما لم تنـل تمويلاً مناسـباً، حتى العام 2012، ولم تحز سـوى القليل من السـلطات. (قدّمت الهيئة تقريراً في 2014، اكتفى بالتركيز على تجميع الوكالة للمعلومات تحت البند 702[43]. وحُظِرَ على نطاق واسع بدعوى أنّه غير مناسب)[44].

يجـب أن يكرّس عدد أكبر من أعضاء الكونغرس أنفسـهم لمهمة إصلاح «وكالة الأمن القومي» بشـكل مفيد. إذ نحتاج إلى إشراف اسـتراتيجي شـامل على الوكالة يكـون متّسـماً بالشـفافيّة التامـة، تنهض بـه وكالات حكوميّـة مسـتقلّة. نحتاج إلى قوانين مؤثّرة من شـأنها تقليص تجميع البيانات عن الأميركيّين وتخزينها، إضافة إلى قوانـين تفرض على الوكالة حذف المعلومات التـي كان يجب ألا تجمعها أصلاً[45]. في سـبعينيات القـرن العشرين، حقّقت «لجنة شـيرش» في عمليـات جمع المعلومات اسـتخباراتياً مـن قِبَل «وكالة الأمـن القومي» والـ «إف بي آي» والــ «سي آي إيه».

واستطاعت إنجاز إصلاح في تلك الأجهزة، بعد بحوث وكشوفات واسعة. نحتاج إلى لجنة كتلك حاضراً. يجب علينا إقناع الرئيس أوباما بتبني التوصيات التي خرجت بها لجنته التي راجعت عمل «وكالة الأمن القومي». ويجب إعطاء سلطات تحقيق فعليّة إلى «هيئة الإشراف بصدد الخصوصيّة والحريّات المدنيّة».

تحمل تلك الاقتراحات كلها دلالة بالنسبة إلى الإشراف الاستراتيجي على الرقابة العامة. إذاً، لننتقل إلى الإشراف التكتيكي. تجسّد عملية الحصول على مذكّرات قانونيّة إحدى الآليات المهمة في الإشراف التكتيكي على الرقابة الحكوميّة. وعلى عكس مزاعم يردّدها بعض المسؤولين الحكوميّين، لا يتأذّى الأمن القومي من المذكّرات القانونيّة؛ بل إنّها آليّة أمنيّة تحمينا من التمدّد الزائد لسلطات الحكومة[46].

ولا تتمتّع الأذونات الأمنيّة السريّة بفعاليّة مماثلة[47]. يأتي القضاة الذين يشرفون على عمل «وكالة الأمن القومي» من محكمة «فيسا» السريّة. وبالمقارنة مع المحاكم التقليديّة، تمتلك «فيسا» مستوى أقل بكثير في الاستناد إلى الأدلة قبل إعطاء إذن أمني. وتضرب ستاراً من السريّة على الحالات التي تنظرها، والأحكام التي تصدرها، كما لا تستدعي أحداً ليمثّل الطرف الآخر أمامها. ومع أخذ عدم التوازن في تلك الآلية بعين الاعتبار، يغدو مدهشاً التماسك الذي أظهرته محكمة «فيسا» في مواجهة الوكالة (على الرغم من أنها لم ترفض إعطاء إذن للوكالة إلا نادراً).

يتخطّى بعض أوامر الرقابة تلك الآليّة كليّاً[48]. إذ لم تتلق مؤسّسة «الاتّصالات الخلوية» في الولايات المتّحدة سوى أمرين قضائيّين للتنصّت على الخطوط، مقابل 10801 مذكّرة تفتيش لم تكن مستندة إلى القضاء إطلاقاً. يجب إصلاح تلك الأمور كلها.

لنبدأ من محكمة «فيسا»: يجب أن تصبح أشد علانية بكثير[49]. يجب أن يتولّى مجلس الشيوخ تعيين كبير القضاة في تلك المحكمة. يجب أن تنشر المحكمة آراءها إلى أقصى حدّ تستطيعه. يفترض تعيين محامٍ للدفاع عن مصالح الجمهور كي يحاجج

ضـد طلبات تطبيق الرقابة. يفترض بالكونغرس أن يسـنّ آلية لاسـتئناف الأحكام الصادرة عن «فيسا»، إما أمام محكمة نقض مختصّة أو المحكمة الفيدراليّة العليا.

هنـاك حاجـة أيضاً لاتخّـاذ مزيد مـن الخطوات لوضـع «وكالة الأمـن القومي» تحـت إشراف تكتيكي موثوق[50]. إذ تميل الإجراءات الداخليّة للوكالة للتلاؤم مع تقصي نشـاطات كالرقابة غير الصحيحة والقابلـة للتجنّب أكثر من اهتمامها بآليات الرقابة التي تسعى إلى كشف من يحاولون التملّص من الرقابة، سواء أكانوا أفراداً أم منظّمات بأكملها. إنّ وجود مراقب خارجي شيء أساسي لتصحيح ذلك. ومن المهم أيضاً أن يضحي الرسـميّون الحكوميّون مسـؤولين بصفة شـخصيّة عن سـلوكيّات الوكالـة المتعديّـة وغـير الشرعيّـة. لم يطـرد متلصّـص مـن مجموعة «لـوف إنت» في الوكالة، ناهيك عن عدم محاكمتهم.

كذلـك صُدّت محاولات سـنودن المتكرّرة داخل الوكالة للتعبير عن قلقه بشـأن المدى الذي بلغته الرقابة على الأميركيّين[51].

تملـك وكالات حكوميّـة أخـرى تعمل عـلى إنفاذ القانـون، كالـ «إف بي آي»، آليـات لـلإشراف الداخـلي[52]. في ذلك المجال أيضـاً، كلما زادت الشـفافيّة تصبح الأمور أفضل[53]. لطالما منحنا الشرطة صلاحيّات اسـتثنائيّة بهدف تقصّي الجرائم. فعلنـا ذلك عن سـابق معرفة، وهو ما جعـل المجتمع أكثر أماناً؛ لأنـه بإمكاننا دوماً ضبـط تصرفات الشرطة بموجب القوانـين، كما يمكن اللجوء إلى أنواع معروفة من التقاضي في حال أساءت الشرطة استعمال سلطاتها. من المستطاع النقاش مطوّلاً عن مدى نجاعة ذلك المسار عمليّاً في الولايات المتّحدة ودول أخرى، لكن تبقى الفكرة الأساسيّة سليمة.

حماية مُطلِقي صافرات الإنذار

يدعم البروفسـور ديفيد بوزن، وهو أستاذ القانون من «جامعة كولومبيا»، فكرة أنّ النُظُـم الديمقراطيّـة يجب أن تكـون مُسَرِّبَة، عادّا التسريبـات وإطلاق صافرات الإنـذار آليات أمنيّـة بحد ذاتها، تتصدى للتوسّـع الفائض في سـلطات الحكم[54]. وكذلك يرى أنّ التسريبات تمثّل نقيضاً لميل السلطات الرسميّة إلى الإفراط في وضع الوثائق في خانة السريّة؛ ما يجعل التسريبات في خاتمة المطاف طريقة لاسـترداد الثقة بالحكومات، بعد تضرّرها من تأثيرات السريّة الزائدة.

كذلك تنظر عالِمَة الإثنيات دانا بويد إلى إطلاق صافرات الإنذار بوصفها شـكلاً للتمرّد المدني في العصر الرقمي؛ لأنّه يعطي قوّة للأفراد في مواجهة إسـاءة استخدام السـلطة[55]. ولاحظت منظمّة «مراقبة حقوق الإنسـان» (Human Rights Watch) غير الحكوميّة، أنّ «الأشـخاص الذين يكشـفون ممارسات رسميّة خاطئة... يؤدّون خدمة جليلة في المجتمع الديمقراطي...»[56].

ووفـق هـذه الطريقـة في التفكـير، يقـدّم مُطلِقـو صافـرات الإنذار آليـة أخرى للإشراف عـلى الحكومة[57]. مـن المسـتطاع اعتبارهم نوعـاً من التفتيـش المفاجئ العشوائي. وعلى غرار القوانين التي تحمي مُطلِقي صافرات الإنذار ضد الشركات، كذلك يجب سـنّ قوانين تحمي مُطلِقي صافرات الإنـذار ضد الحكومة[58]. ولدى إقرارها، نحصل على إطار وقوانين لإطلاق صافرات الإنذار بطريقة شرعيّة[59].

ولا يعنـي ذلك أن يضحي كل شـخص حرّاً في تسريـب وثائق حكوميّة بدعوى أنّـه مُطلِـق صافـرة إنـذار. في المقابـل، يعني ذلـك تماماً أن كشـف أخطـاء الحكومة بدافـع مـن الضمـير، يمكن اتّخـاذه سـنداً قانونيّاً يسـتخدمه مُطلقو صافـرة الإنذار عنـد مثولهـم أمام المحاكم- يبقى على القضاة الحكم عـلى صحة مبرّراته- إضافة إلى تمكينهـم من الحفاظ على سريّة مصادرهم. هناك نقطة ذكيّة في هذه الصيغة تتمثّل في تنحيـة الإشـكاليّة الصعبة التي يشـكّلها تعريف «مُطلِق صافرة إنـذار»، إضافة إلى

تمكين المحاكم من التحديد في كل حال على حدة، الأفعال التي ينطبق عليها ذلك الوصف[60]. بذا، يستطيع شخص كسنودن أن يعود إلى الولايات المتّحدة ويقدّم قضيّته إلى المحاكم[61]، وهو أمر يتعذّر عليه حاضراً وفق ما بيّنتُ في الفصل 7.

إضافة إلى ذلك، نحتاج إلى سنّ قوانين تحمي الصحافيّين في حال تمكّنهم من الوصول إلى معلومات مصنّفة سريّة. إذ لا يمثّل كشف الأمور علانية عملاً تجسسيّاً بحد ذاته، ومعاملة الصحافة كأنها جاسوسيّة أمر مؤذٍ للديمقراطيّة، بطريقة تفوق المألوف تماماً.

في الفصل السابع، تحدّثت عن حماسة فائضة لدى إدارة أوباما في اضطهاد مُطلِقي صافرات الإنذار. تجمع تلك سياسة الرياء والخطورة معاً. إذ نشجّع الأفراد على إطلاق صافرات الإنذار بشأن تجاوز القانون مِنْ قِبَل القطاع الخاص، ولكننا نحتاج إلى قوانين مماثلة بشأن الحكومة أيضاً[62].

تضييق الاستهداف وحصره بالموافقة القانونيّة

تشكّل الرقابة الإلكترونيّة أداة قيّمة بالنسبة لقوى إنفاذ القانون وتجميع المعلومات الاستخباراتيّة معاً، لذا يفترض أن نستمر في استخدامها. هناك مشكلة في فرض رقابة إلكترونيّة على أمّة بأكملها، خصوصاً الرقابة العامة التي لا تتقيّد بأوامر القضاء. وكما رأينا في الفصل 11، لا تجعلنا تلك الرقابة أكثر أماناً. وفعليّاً، إنّها تقلل من أمننا بأنّها تحرف الاهتمام والأموال عن الوصول إلى أشياء تجعلنا أكثر أمناً حقاً. يتمثّل الحل فعليّاً في العودة حصريّاً إلى الرقابة الموجّهة.

وفق كلمات آكسل آرنباك وهو باحث في القانون والأمن السبراني، يتحكّم القانون بالأبواب الأماميّة، وتسيطر نظرية الألعاب(*) على «الأبواب الخلفيّة»[63].

(*) في أربعينيات القرن الماضي، صاغ عالِم الرياضيّات الأميركي جون ناش نظرية عن حساب المخارج المحتملة لأشكال متنوّعة من الصراعات، تشمل الاقتصاد والجيوش والاقتصاد والعلاقات الاجتماعيّة.

وقصد آرنباك القول إنّ عملية الرقابة الموجّهة تتحكّم بها عناصر كالسبب المحتمل، المذكّرات القضائيّة، محدوديّة الإطار وغيرها من القوانين التي تحمي أمننا وخصوصيّتنا. وتتحكّم بالرقابة العامة التحليلات الباردة عما تستطيع المؤسّسة جمعه من المعلومات، وطُرُق الإفلات من تبعات ذلك. عندما نعطي «وكالة الأمن القومي» القدرة على تنفيذ رقابة عامة بالتملص من آليّة المذكّرات القضائيّة، نتيح لموظفي الوكالة التفكير أكثر في ما يستطاع جمعه من معلومات، والتفكير أقل في مدى قانونيته. عندها، نفسح لهم المجال ليكونوا طمّاعين ومتعجرفين؛ وندفع ثمن ذلك.

تقلب رقابة المجاميع عملية التحقيق التقليديّة رأساً على عقب. وفي ظلّ الإيقاع الطبيعي للعمليات، لا بد لقوى إنفاذ القانون من سبب كي تشتبه بشخص ما، وكذلك لتتقدّم بطلب مذكرة قضائيّة لوضعه تحت الرقابة. وتفسح رقابة المجاميع المجال أمام قوى إنفاذ القانون لرقابة الجميع- وصنع أرضيّات للاشتباه. إنّها أمور نص الدستور الأميركي صراحة على منعها، ولأسباب وجيهة تماماً. ولذلك أيضاً، استنتج تقرير الأمم المتّحدة في 2014 أنّ الرقابة العامة تهدّد القانون الدولي(64).

نحن بحاجة إلى تشريعات ترغم وكالات الاستخبارات وقوى إنفاذ القانون على جعل رقابتهم موجّهة؛ بل نحتاج إلى سنّ تشريعات جديدة وتدعيم التشريعات القائمة معاً سويّة. بفضل ذلك المزيج، تحصل قوى إنفاذ القانون على ما تحتاجه من معلومات بصورة محدّدة، وكذلك تحصل الوقاية من إساءة استخدامها.

خطّت المحكمة العليا في أميركا خطوة طفل صغير في ذلك الاتّجاه في 2013، عندما اشترطت حصول ضبّاط الشرطة على مذكّرة قضائيّة قبل وضع أداة إلكترونيّة مرتبطة بنظام الـ «جي بي إس» في سيّارة المشتبه فيهم(65)، وتلتها خطوة أخرى في 2014 باشتراط حصول ضباط الشرطة على مذكرة قضائيّة لتفتيش الهاتف الخلوي للموقوفين والمعتقلين(66).

في الولايـات المتّحدة، نحتاج إلى التخلّـص من نظام الطرف الثالث المتقادم[67]، وأنّ نقرّ بأن المعلومات تبقى محتفظة بكونها شـخصيّة حتى لو جرى إيكالها إلى أحد المُقَدّمين الموثوقين لخدمة الإنترنت. يجب أن تضطر الشرطة إلى الحصول على مذكرة قضائيّة للوصول إلى بريدي الشخصي، سواء أكان مكتوباً على الورق أم إلكترونيّاً في حاسوبي في المكتب أم في خوادم شركة «غوغل» أينما كانت في العالم[68].

يملـك الكثير من تلك الأشـياء طابعاً دوليّاً. ويتطلّب إنجـاح ما اقترحته أنّ تقرّ الحكومـات بأنهـا ملزمَة بحماية حقـوق مواطنيهـا وحرياتهم، بل حقـوق المواطنين وحرياتهـم عالميّـاً. إنّه أمر مسـتجد تمامـاً؛ ذلك أن الحمايـات القانونيّـة في الولايات المتّحـدة حيـال الرقابـة، لا تنطبق على غـير الأميركيّين خارج تلـك البلاد. يفترض وضع اتفاقيّات دوليّة تأخذ بعين الاعتبار أن واجبات بلد ما لا تتوقّف عند حدوده. هناك مسـوّغات أخلاقيّة أساسـيّة للقيام بذلك، إضافة إلى وجود أسـباب براغماتيّة لـه. إذ تسـاعد حماية حق الأجانـب في الخصوصيّة في حماية حقوقنا أيضـاً، كما تتأتى الأضرار الاقتصاديّة التي ناقشتها في الفصل 9 من إيذاء تلك الحقوق.

لنصلح معظم الثغرات

وفـق مـا ناقشـته في الفصـل 11، ثمة نقـاش جارٍ حـول وجوب قيـام الحكومة الأميركيّة- تحديداً «وكالة الأمن القومي» و«القيادة العسـكريّة للفضاء السبراني»- بتجميـع ثغرات النُظُم الإلكترونيّة، أو العمل على إصلاحها وسـدّها. إنها مسـألة معقّـدة تمامـاً، وتعطي نموذجاً سـاطعاً عـن صعوبة الفصل بين الهجـوم والدفاع في الفضاء السبراني.

ثمـة سـباق تسـلّح مندلـع في الفضاء الافـتراضي للإنترنـت حـاضراً. إذ يعمل الصينيـون والروس وغيرهم على تكديس سـجلات عن الثغرات في المواقع والنُظُم الإلكترونيّـة[69]. إذا تركنـا الثغـرات مفتوحـة، فلربـما اسـتطاع بلـد آخـر كشـفها باستقلاليّة، ما يعطيه القدرة على استغلالها ضدنا وضد حلفائنا. في المقابل، إذا عملنا

على ســدّ الثغرات كلها، نفقد سـلاحاً مهمّاً لأننا لن نتمكن من اسـتغلال ثغرات في توجيه ضربة ما في الفضاء السبراني ضد عدو محتمل.

يعتقد بعض الناس أنّ «وكالة الأمن القومي» يجب أن تكشف وتصلح الثغرات *كلهـا*[70]. ويزعم آخرون أنّ ذلك يشـبه نزع سـلاح من طرف واحـد[71]. أوصت لجنـة الرئيـس أوبامـا للتدقيق في «وكالة الأمن القومي» بما يشـبه حلاً وسـطاً: يجب ألا تكـدّس الثغـرات إلا نادراً، ولفترة قصيرة[72]. أَثَرتُ تلك النقطة بنفسي[73]. إذ إنها عين ما تزعم الوكالة، واسـتطراداً «القيادة الأميركيّة للفضاء السـبراني»، أنها تفعلـه[74]: إيجـاد توازن بـين عوامل متنوّعة تشـمل إمكان أن يكتشـف طرف آخر تلك الثغرات (راجع النقاش عن «نوباس» في الفصل 11)، والأهمية الاستراتيجيّة لذلـك الأمر بالنسـبة للولايـات المتّحدة. في المقابل، تشـير الأدلة إلى أنّ ما تكدّسـه الوكالة من الثغرات يفوق كثيراً ما تعلن عنه.

تمثّـل تلك الحال خطوة إلى الخلف. يجب أن يكون خطأنا في طرف الكشـف عن الثغـرات. إذ يسـاعد ذلك البلـدان التي تعتمـد بكثافة على البنيـة التحتيّة للإنترنت كالولايات المتّحـدة. ويعيد ذلك الثقة بالولايات المتّحدة بإظهارها رغبتها في وضع الأمن قبل الرقابة. وفي ما يُحتَفَظ بالثغرات وسـجلاتها سرّاً، يكون من الأفضل فتح نقاش عن نوع الثغرات التي يجب الإبقاء عليها. ويتطلّب إنجاز ذلك بكفاءة، وجود منظّمة حكوميّة مستقلّة تملك خبرات تقنيّة ملائمة في اتّخاذ القرارات.

في السـباق على التسـلّح الجاري حاضراً، تستثمر المؤسّسـات العسكريّة أموالاً أكثر في البحث عن الثغرات وكذلك في شراء المعلومات عنها، بأكثر مما يوظّف عالم التجارة أموالاً في إصلاحها. يحمل تكديس الثغرات وسـجلاتها خطراً علينا جميعاً. وبغض النظر عمّا يفعله مجرمو الفضاء الافتراضي، وما تفعله البلدان الأخرى، يجب على أميركا نقل الخلل إلى الجانب الأمني بإصلاح معظم الثغرات التي نكتشفها، مع

جعل عملية كشفها أكثر علانية. سيجعلنا ذلك أكثر أمناً، مع توليد الثقة بسياسة الولايات المتّحدة والمرتكزات التقنيّة للإنترنت معاً.

لا تخرّب المنتجات والمعايير

تمتلك الثقة أهميّة حاسمة للمجتمع؛ وهي شخصيّة، نسبيّة، وضعيّة وسيّالة. وتستند عليها إنجازات الشعوب كافة. يجب أن نكون قادرين على الثقة ببعضنا بعضاً، وبمؤسّساتنا الحكوميّة والخاصة، وبالنُظُم التكنولوجيّة التي تؤمن وظائف المجتمع. وعندما نبني نُظُماً، نحتاج إلى التأكّد من كونها أهلاً للثقة بمثل كونها فعّالة.

وتبدو طبيعة الثقة بالإنترنت أمراً مثيراً للاهتمام. إذ لا يملك المتمرسون بالتقنيّة أوهاماً بشأن أمن الإنترنت وقدرة الحكومات والمجرمين والـ «هاكرز» وغيرهم على اختراق الشبكات، طالما امتلكوا الدافع والقدرة على ذلك. لا نثق أبداً بأن المبرمجين لا يرتكبون أخطاءً، وأن الشيفرة خالية من العيوب، ولا حتى بمناعة المعادلات الرياضيّة للشيفرة التي نصوغها بأنفسنا.

إذ نعرف جيّداً أن أمن الإنترنت هو سباق تسلّح، والمهاجمون يمتلكون معظم الأفضليّات.

إن ما نثق به حقاً هو أن التقنيّات تصمد أو تنهار ارتكازاً إلى ميّزاتها الخاصة. وبفضل كشوفات سنودن، بتنا نعرف أن تلك الثقة كانت في غير موضعها. وللسبّب عينه، ولّدت برامج الرقابة لـ «وكالة الأمن القومي» و«القيادة الحكوميّة للاتّصالات»، احتجاجات واسعة عالميّاً؛ وثار غضب المجتمع التقني على نحو خاص بسبب ما كشفته وثائق سنودن من تعمّد الوكالة تخريب معايير الإنترنت ومنتجاتها وبروتوكولاتها[75]. لقد أضعفت برامج الوكالتين الأميركيّة ونظيرتها البريطانيّة الثقة بالتقنية التي تستند إليها الإنترنت.

ناقشتُ في الفصل 6، محاولات الـ «إف بي آي» المستمرة للحصول على قوانين تفرض وضع «أبواب خلفيّة» خدمة للأمن[76]. وناقشت في الفصل 11، كيف عمدت «وكالة الأمن القومي» سراً إلى دسّ «أبواب خلفيّة» في منتجات الإنترنت وبروتوكولاتها، بما يمكّنها من ممارسة التجسّس. ويفترض أن يذهب بنا الظن إلى أنّ بلداناً أخرى مارست الشيء نفسه مع منتجاتها (ومع بعضها بعضاً)[77]. واستنتج مراقبون أن شركات لديها طواقم تطوير إسرائيليّة، كـ «فِرينت» (Verint) و«نارنت» (Narent) و«آمدوكس» (Amdocs)، تنام في السرير عينه مع الحكومة الاسرائيليّة، وأنّ معدّات شركة «هواوي» (Huawei) متّصلة بـ«أبواب خلفيّة» مع الحكومة الصينيّة[78]. هل نثق بالمنتجات الأميركيّة المصنوعة في الصين؟ هل نثق بالمواطنين الإسرائيليّين العاملين في شركة «مايكروسوفت»؟ هل نثق بالمُكوّنات الإلكترونيّة والبرامج الرقميّة المصنوعة في روسيا؟ فرنسا؟ ألمانيا؟ هل نثق بأي شيء مصنوع في أي مكان؟

إنّ غياب الثقة سمّ. يجب أن تعطى الأولويّة للأمن، وبعده يأتي التنصّت[79]. تستطيع قوى إنفاذ القانون الحصول على مذكرة قضائيّة لممارسة التنصّت، لكن يجب ألا يكون بمكنتها إرغام شركات الاتّصالات على ضمان نجاح كل محاولاتها في التنصّت. يجب استرداد تشريع «كاليا» [الاسم المختصر لـ «قانون مساعدة الاتّصالات في إنفاذ القانون»(*)] وتفعيله بما يجعله يعمل على ضمان أمن شبكات الهاتف والإنترنت.

سيحاول العاملون في قوى إنفاذ القانون على تلك الأمور كلها تخويفنا، باستعادة رؤى الخاطفين والمتغولين جنسيّاً على الأطفال، وتجار المخدّرات، وإفلات الحبل على غاربه للإرهابيّين؛ لأن قوى إنفاذ القانون لم تعد قادرة على كسر شيفرات كومبيوتراتهم واتّصالاتهم. رأينا ذلك في أواخر العام 2014 عندما لجأت شركة

(*) راجع الفصل السادس.

«آبل» إلى تشفير معلومات «آي فون». وحينها، عمد مسؤولو قوى إنفاذ القانون، واحداً تلو الآخر، إلى إثارة أشباح الخاطفين والمعتدين على الأطفال[80]. كانت محاولة متعمّدة للعب على وتر الخوف، لكن أحداً من أولئك المسؤولين لم يشر إلى قضيّة بعينها عن حدوث أيٍّ من تلك الأشياء. ومن أصل 3576 اعتداء كبيراً جرى منح أذن قانوني بالتنصّت أثناء التحقيق فيها سنة 2013، ظهرت قضية خطف وحيدة لكن ضحيتها لم يكن طفلاً[81]. والأهم لم يظهر دليل على أن التشفير يعيق جديّاً التحقيقات في الجرائم، بأي طريقة كانت[82]. في 2013، ضلّل التشفير الشرطة 9 مرات، بزيادة 4 حالات عن 2012، لكن التحقيقات تواصلت بطرق أخرى.

تملك قوى إنفاذ القانون مروحة كبرى من الأدوات الاستقصائيّة. وتستطيع الحصول على مذكّرات قضائيّة للوصول إلى البيانات المخزّنة في السحب الرقميّة، ومجموعات ضخمة من «البيانات الوصفيّة». إنّها تحوز القدرة والحق للتسلّل إلى حواسيب المشتبه فيهم، بغية الوصول إلى المعلومات التي تحتاجها من دون إضعاف أمننا جميعاً[83]. إنّ الأمن الجيّد لا يعرضنا للمخاطر.

يجب على مؤسّساتنا الأمنيّة ألا تزرع ثغرات في أي شيء سوى نُظُم محدّدة تملكها الحكومات والقوى العسكريّة الأجنبيّة، سواءً سراً أم علانية، كما يجب عليها التعاون مع المؤسّسات الأكاديميّة ومجتمعات الأعمال كي تضمن أن الثغرات التي تزرعها أطراف عدوانيّة سوف تُكشف ويُعلن عنها ويُبطل عملها.

لن نتوصل إلى توافق مع قوى العالم كلّها على عدم تخريب الجزء الذي تسيطر عليه من الإنترنت، لكن يجب علينا التوقّف عن تخريب الأجزاء التي تقع تحت سيطرتنا. تضمّ الولايات المتّحدة غالبية الشركات التي تسيّر عمل الإنترنت، ما يعطي أميركا نفوذاً لا يضارع. وبمجرد توقّفنا عن لعبة التخريب، نستطيع توجيه

مواردنـا بشـكل موثـوق إلى تقصي التخريـب الذي يحدثـه آخـرون ومكافحته على الإنترنت، ما يزيد مستويات الثقة عالميّاً.

فصل التجسّس عن الرقابة

في العام 2013، علمنا أن «وكالة الأمن القومي» تجسّست على هاتف المستشارة الألمانيّـة أنغيلا مـيركل[84]. علمنا أن الوكالة تجسّسـت على سـفارات وبعثات على امتـداد العـالم: البرازيـل، بلغاريـا، كولومبيا، الاتحـاد الأوروبي، فرنسـا، جورجيا، اليونان، الهند، إيطاليا، اليابان، المكسيك، سلوفاكيا، جنوب أفريقيا، كوريا الجنوبيّة، تايوان، فنزويلا، فيتنام[85]. علمنا أيضاً أن الوكالة تجسّست على الأمم المتّحدة[86]. بالطبع، أرخت تلك الكشوف ظلالها على العلاقات الدوليّة، لكن هل فاجأت أحداً فعليّاً؟ إنّ التجسّس على الحكومات الأجنبيّة هو عين ما يفترض بالوكالة أن تفعله.

إنّ التجسّـس المتبـادل بـين الحكومـات قديم قِـدَم الحكومات نفسـها. إنّه عمل عسكري مهم في أوقات السلم والحرب، وسوف تستمر أبداً. إنّه عمل موجّه أيضاً. وعمليّاً، يسـاهم ذلك في الاسـتقرار لأنّه يزيل شـكوكاً متبادلة عن نوايا الدول تجاه بعضها بعضاً[87].

هنـاك فـارق كبير بين التجسّـس الذي تمارسـه «وكالة الأمن القومـي» من جهة وبرامجها في الرقابة العامة أميركيّاً ودوليّاً من الجهة الثانية. في الفصل 5، لاحظتُ أنّ تلك النقلة في مهمة الوكالة نجمت من نقلة في مهمّتها بشأن مكافحة الإرهاب. فبعد 11/9، أنيـط بتلـك الوكالة المهمة الرئيسـة في الرقابة المتعلّقـة بمكافحة الإرهاب؛ لأنّهـا تمتلك القدرات المطلوبة لتلك المهمة فلا يزيـد الأمر على إعادة توجيهها، على الرغم من أن تلك المهمّة كان من المستطاع إسنادها إلى الـ «إف بي آي».

ومـع توليها مهمة الرقابـة لمكافحة الإرهاب، توسّـعت قواعد عملها عسـكريّاً والإطـار القانوني المتّصل بنشـاطاتها الأساسـيّة في التجسّـس. وبـذا، وجب فرض

السريّـة بشـأن ممارسـتنا الرقابة على شـعوب بأكملها (ومن بينها شـعبنا)، تسـاوي السريّة المفروضة على نشاطاتنا التجسّسيّة ضد الحكومات.

نحتـاج إلى فصـل هاتـين المهمتين عـن بعضهما بعضـاً. يجب أن يبقى التجسـس الحكومـي تحـت إشراف وزارة الخارجيـة والمؤسّسـة العسـكريّة. يفـترض أن يناط بالرئيـس بوصفـه القائد الأعـلى، تقريـر السـفارات والهواتف التي يجـب التنصّت عليهـا، كما يفـترض بـ «وكالة الأمن القومـي» تنفيذ أوامره. ويجـب ألا تبرّر غالبية أعمال الرقابة العامة، سواء داخل الولايات المتّحدة أم على الأجانب. أحياناً، يمكن تبريـر رقابة الحكومة لمواطنين بعينهم، لكن يشـترط أن يجـري ذلك ضمن تحقيقات جرميّة حصريّاً. ويجب نقل نشـاطات الرقابة العامة خارج إطار الوكالة والمؤسّسـة العسـكريّة. يفـترض بتلك النشـاطات أن تكون تحت إمرة الـ «إف بي آي» ووزارة العدل اللتين تتقيدان بقواعد عمل الشرطة على غرار وجود قضيّة محتملة، التزام آليّة مناسبة والإشراف على نشاطات الرقابة، ضمن أطر المحاكم العادية العلنيّة.

لا يعنـي ذلـك أن الولايـات المتّحـدة ليسـت بحاجـة إلى إصلاح ضخـم لعمل الشرطـة. ولقـد ناقشـت في الفصـل 7 مسـألة سريّـة الشرطـة. ثمة مشـكلة كبرى تمثّلها العسـكرة المتزايدة للشرطة، وكذلك ميل وزارات كثيرة إلى ممارسـات تمييزيّة جذريّـة[88]. وتصلح تلك الأمور موضوعـاً لكتاب آخر[89]. إنّ مكافحة الإرهاب كانت ولا تزال، هي المهمّة الرئيسة للـ «إف بي آي».

في كانـون ثـاني (يناير) 2014، ألقـى الرئيس أوباما خطاباً بشـأن «وكالة الأمن القومي»، أثار فيه نقطتين بالغتي الأهمية. إذ وعد ألا تسـتمر الوكالة في رقابة هاتف أنغيـلا مـيركل. وعلى الرغـم من أنه لم يوسّـع تلك الهبة لتشـمل بقية الـــ82 مليون مواطن ألماني، فإنه أعلن أنه قد يوسّـع بعض الحمايات التي يؤمّنها دسـتور الولايات المتّحـدة حيال الرقابة غير المبررة، كي تشـمل بقية العـالم[90]. وإلى حدّ كبير، يتلاءم

تحقيـق هذا الهدف مع وضع رقابة الحكومة على الشـعب تحت إشراف مدني، إضافة إلى تقييدها بقواعد عمل الشرطة.

تنظيم دور العسكر في الفضاء السبراني

مثّـل فصـل الحكومة المدنيّة عن العسـكر إحـدى الإنجازات الكـبرى في الهزيع الأخـير من القرن التاسـع عشر. وبرهن التاريخ والحوادث السياسـيّة المعاصرة معاً عـلى الدمـار الهائل الـذي يحيق بالمجتمع حين يتـولى الجنرالات أمـر البلاد. وأعطى الفصل بين السـلطتين المدنيّة والعسـكريّة، وهو ما فعلته بلدان كثيرة عالميّاً، مسـاحة لازدهار الديمقراطيّة والحريّة.

تتجسّـد المشـكلة في أن الفضاء السـبراني لا يسـتطيع بسـهولة الفصل التقليدي بين المجالين العسـكري والمدني. عندما تتعرّض لاعتداء جسـدي، تلجأ إلى منظّمات كثيرة للدفاع عنك كالشرطة والجيش وكل من يسـتطيع الدفاع عنك ضد الإرهاب في بـلادك، إضافـة إلى محاميك. يعتمد النظام القانـوني في تبريره تلك الدفاعات على مرتكزيـن: مـن يهاجمـك، ولماذا. للأسـف، عندمـا تُهاجَـم في الفضاء السـبراني فإنّ الشيئين اللذين لا تعرفهما هما من يهاجمك ولماذا[91].

إضافـة إلى ذلـك، لا تملـك الإنترنـت حـدوداً تقـارن بالحـدود الفعليّـة بـين الـدول[92]- بـل يمكنـك القول إنـه لا حدود لها إطلاقـاً- لذا يصعـب التمييز بين الشـأنين الداخـلي والخارجي فيها. إذ تشـمل مروحة من يشـنون الهجمات مراهقين يسعون لتزجية أوقات الفراغ، ومنظّمات إجراميّة محترفة، وحتى الدول ومؤسّساتها، وربما استخدموا جميعهم التكتيكات والأسلحة عينها، ما يجعل من الصعوبة بمكان التمييـز بـين أنواع المهاجمين. تحـدث الهجمات خلال كسـور من الألف مـن الثانية، وتخلّف آثاراً متنوّعة.

ويتمثّل ردّ الفعل على ذلك بجمع المهاجين كافة تحت مسمّى «الحرب السبرانيّة»، وهو أمر جديد وجدّي بالنسبة للتخطيط العسكري. وذكرت سابقاً أنّ قرابة 30 بلداً لديها فرق في جيوشها مكرّسة للحرب السبرانيّة. وثمة عقلية آخِذة بالبزوغ تسمّى «الحصار السبراني»(93).

مع ملاحظة أنّ ذلك المسرح الحربي هو جديد ومجهول، وكل ما يحدث فيه يجري بسرعة هائلة، وتذكّر ميل العسكر إلى التمسك بكونهم على حقّ دائماً؛ لأنّهم يؤدّون مهمة ما، مهما كانت صيغتها؛ هرعت الجيوش كي تملأ ما بدا لها فراغاً أمنيّاً. وترافق ذلك مع انتشار انطباع بأن هناك مشكلاتِ عسكريّة، وتبحث عن حلول عسكريّة. وفي أسوأ الأحوال، تميل إلى التوتاليتاريّة [الشموليّة]، وتكون غير شرعية في أفضل الأحوال(94).

يجب إصلاح ذلك تماماً.

في الولايات المتّحدة، هناك سلسلة من القوانين التي تحول دون تدخّل العسكر في الشؤون المدنيّة أيام السلم، مع ضمان جهوزيتهم للتصدي للتهديدات الخارجيّة. في العام 1878 ظهر «قانون بوزيه كوميتاتوس» (Posse Comitatus Act) (95)، ثم تلته تشريعات أخرى، لمنع العسكر من الانخراط في شؤون الأمن الداخلي. ولأننا قصرنا دور العسكر على الحرب ضد قوى خارجيّة، أنسنا إلى إعطائهم هوامش أكبر في الحركة. ومثلاً، لا تنطبق قوانين المصادرة والتفتيش المفروضة على قوى إنفاذ القانون على العسكر؛ لأنه ببساطة ليس منطقيّاً تطبيقها في غمار الحرب.

يجب أن تبقى العمليات العسكريّة الهجوميّة في الفضاء السبراني تحت إشراف العسكر، سواء أكانت تجسّساً أم هجمات. في الولايات المتّحدة، يترجم ذلك بـ «القيادة السبرانيّة الأميركيّة» (US Cyber Command) (96). إذا كنّا بصدد الهجوم على البنية التحتيّة الإلكترونيّة لبلد آخر، يجب التعامل مع ذلك كأي هجوم عسكري على بلد آخر. لا يتعلّق الأمر بالتجسّس العادي (سواء في العالم السبراني أم الفعلي)،

بـل بالهجـوم. يجـب النظـر إلى تلك الهجـمات السـبرانيّة بوصفهـا أعمالاً عسـكريّة هجوميّة، ما يعني أيضاً وجوب إقرارها على أعلى مسـتويات السـلطة التنفيذيّة، كما يجـب خضوعهـا لمعايير القانون الدولي عينها التي تنطبق عـلى الحرب الفعليّة خارج الفضاء السبراني.

تقسيم «وكالة الأمن القومي»

بموجـب الكلمات السـابقة، اقترحـت الفصـل بين مهمّتي الوكالة في التجسّـس والرقابـة، وأن يقيّـد دور العسـكر في الفضـاء السـبراني بالأعمال التي تطـال أهدافاً عسكريّة أجنبيّة. ولإنجاز ذلك، أؤيّد تقسيم الوكالة مع تعزيز مسؤولياتها كافة التي كانت مناطة بها قبل 9/ 11:

* بوصفهـا جـزءاً مـن وزارة الدفـاع، يجـب أن تبقـي الوكالـة تركيزها على التجسّس على الحكومات الأجنبيّة.
* يجب أن تتولّى وزارة العدل المسـؤولية عن قوى إنفاذ القانون والتحقيقات المتّصلـة بالإرهـاب. ولذا، يفـترض أن يقتصر أمرها عـلى الرقابة الموجّهة والمجازة قانونيّاً، سواء أكانت داخليّة أم خارجيّة؛ إضافة إلى توليها متابعة الأدلة المسـتندة إلى خبرات ضبّاط الـ «إف بي آي»، وليس قواعد البيانات في «وكالة الأمن القومي».
* يجـب إبـراز القـدرات الدفاعيّـة التـي تمتلكهـا الوكالة في التشـفير، وأمن الكومبيوتر، والدفاع عن الشـبكات؛ مع جعلهـا علنيّة أكثر[97]. يجـب أن تُحكَـم قبضة «المعهد الوطني للمعايير والتكنولوجيا» (National Institute of Standards & Technology) ويُعرف باسـمه المختصر «نيسـت» (NIST)، هـو وكالـة مدنيّة تعمل خـارج وزارة الدفاع على تطويـر المعايير التقنية في أمـن الشـبكات. إذ حـاول «قانون أمـن الكومبيوتـر- 1987»[98] إبقاء «وكالة الأمن القومي» خارج إطار الأمن المحلي بتوضيحه أن «نيسـت»- حينهـا، كان اسـمها «المكتـب القومـي للمعايـير» (National Bureau of

(Standards –تتولى القيادة في إرسـاء معايير الأمن التقني. نحتاج إلى تمتين ذلك القانون والتأكّد من الالتزام به.

* يجـب إبقاء القدرات الهجوميّة في الفضاء السـبراني بيد «القيادة السـبرانيّة الأميركيّـة»، التي يجب أن تحوز القدرة على اخـتراق نُظُم الكومبيوتر التي تملكها «وكالة الأمن القومي»، (تسـمّى اختصاراً «تاو»). كذلك يجب ألا يتولى مدير الوكالة منصب القيادة في «القيادة السبرانيّة الأميركيّة».

مـن الواضح أنها خطّة واسـعة المـدى، لكنها الخطة الصحيحـة. وأثناء تنفيذها، يجـب خفض تمويل «وكالة الأمن القومي» إلى المسـتوى الذي كانه قبل 9/ 11. من شأن ذلك بحد ذاته أن يترك آثاراً طيّبة.

مكافحة الحركة باتجاه السيادة الوطنيّة في الفضاء السبراني

قبل عشرين عاماً، لم تحز سوى قلّة من الدول قوانين تتحكّم بالإنترنت. وحاضراً، تملك معظم الدول قوانين مشابهة، بل إن بعضها فائق القسوة. لا يبدو ذلك مفاجئاً لأن الإنترنت باتت شـيئاً فائق الأهمية فلا تسـتطيع الحكومات تجاهلها. لكن بعض متابعي شؤون الإنترنت يدهشون من ذلك التحوّل، بل يبقون على دهشتهم أيضاً.

باطّـراد، تحـارب حكومات عدّة الطبيعة العالميّة المتأصّلة في الإنترنت. إذا سـعى حاكم لرقابة شـعبه، والحدّ مما يسـتطيع قراءته، ولجم ما يقولـه؛ عندها يمثل الطابع العالمي المفتوح للإنترنت مشكلة فعليّة لذلك الحاكم.

وبسـبب ذلك، ساندت حكومات كروسـيا والصين والسعودية لسنوات طويلة فـرض رقابـة وطنية على الإنترنـت ضمن تلك البلاد. وبواسـطة مؤسّسـات دوليّة كـ «الاتحـاد الـدولي للاتّصالات»، وهو مؤسّسـة تابعـة للأمم المتّحـدة تتولى وضع معايـير الاتّصـالات التليفونيّـة؛ صارعت تلـك البلدان ضد الإبقـاء على الإنترنت بيـد منظّمات غير رسـميّة تملكها أطراف متعدّدة، وهو الوضـع القائم حاضراً. تبدو

محاججات تلك الدول حميدة، لكن دوافعها ليست كذلك. إذ يريدون للإنترنت أن تقرّ بالحدود الوطنيّة، وبحق الحكومات في التحكّم بها ضمن تلك الحدود أيضاً، ما يولّد مزيداً من الرقابة والحجب[99].

أعطى الكشف عن نشاطات «وكالة الأمن القومي» في الرقابة تدعيماً ضخماً لتلك المقاربة. قاومت حكومات كثيرة الهيمنة الأميركيّة على الإنترنت انطلاقاً من خشيتها على خصوصيّة مواطنيها. إذ دعت حكومات كالبرازيل[100] وألمانيا[101] إلى تخزين معظم معلومات مواطنيها ضمن حدودها. وهناك حكومات لديها أجندات معاكسة، لكنها تذرّعت بذلك الخطاب عينه. وسنّت روسيا قانوناً في 2014 يفرض على الشركات العاملة على الشبكة أن تخزّن معلومات مواطنيها ضمن حدود بلادهم، فتكون خارج متناول «وكالة الأمن القومي» لكنها طوع يد الحكومة الروسيّة[102].

لديّ آراء متضاربة في ذلك الشأن. فمن جهة، أرغب في رؤية قوانين قويّة في حماية خصوصيّة المواطنين تعمّ الدول بطلب الأخيرة وضع المعلومات ضمن سلطاتها القانونيّة. ومن الجهة الثانية، لا أعتقد أن ذلك يحمي تلك البيانات من رقابة الوكالة. ففي الداخل الأميركي، هناك على الأقل بعض من القيود على ما تستطيع الوكالة الوصول إليه. لكن، إذا خزّنت المعلومات في خوادم في ألمانيا والبرازيل، تزول تلك العوائق. ومع معرفة القدرات التقنيّة التي تحوزها الوكالة، لا يخامرني شكّ في أنها ستستطيع الوصول إلى تلك المعلومات على كل حال.

يعطي الطابع الدولي الأصيل في الإنترنت مغانم كثيرة للشعوب التي تعيش في بلدان يسودها الرقابة والحجب. غالباً ما تكون السيادة السبرانيّة مجرد ستار دخان يخفي رغبات السياسيّين في رصد مواطنيهم ورقابتهم، من دون تدخّل شركات أو حكومات أجنبيّة. وكذلك ينظر إلى القتال ضد السيادة السبرانيّة بوصفها ستار دخان يخفي جهود «وكالة الأمن القومي» في كسب نفاذ أوسع إلى الاتّصالات

العالميّـة. يجـب علينا [الأميركيّـين] تجديد تمسـكنا بدعم حرية الإنترنـت وانفتاحها وعالميّتها، ثم العمل على استمرارية وجودها بوصفها كذلك.

إعطاء الجمهور العام

تحوز الفضاءات العامة غير المملوكة فوائد اجتماعيّة جمّة. إذ لا تملك جهة خاصة أرصفتنـا وطرقنـا ومنتزهاتنـا العامة، بـل هناك قوانين تبـيّن أنّ ملكيّتهـا عامة. على الإنترنت، ترجع ملكيّة الأشـياء كلها إلى جهـات خاصة، حتى الموقع الخاص الذي يديره صديقك هو مستضاف على خوادم لشركة ما. لا ملكيّة للعامة.

ليـس ذلك هو الانطباع الذي نملكه عن تجربتنا في اسـتخدام الإنترنت[103]. إذ تبدو الثرثرة عبر «فيسـبوك» كأنها حديث شـخصي، وتتملكنا الدهشة عندما تمارس تلـك الشركـة حقوقها في حذف تدوينات ومنع أشـخاص. وتتزايد دهشـتنا عندما نعلم أننا لا نملك الحق في مقاضاتها، بل ولا حتى في بياناتنا. نعم، لقد سـلّمنا تلك الحقوق إلى الشركة عندما ضغطنا على زر الموافقة على الاتفاقيّة مع المستخدم. ولأننا لم نهتم بقراءتها فعليّاً، لم نكن على معرفة كافية بها[104].

تكتسـب الأمكنة العامـة على الإنترنت أهميتها من واقع أن كثـيراً من حريّاتنا في العـالم الفعلي تكـوّن في أمكنـة عامة. في الولايـات المتّحدة، يحمي التعديل الأول في الدسـتور حق التعبير في الأمكنة العامة. هناك قوانين أخرى تحظر نشاطات كالسكر والعربـدة في الأمكنـة العامـة. لا تنطبـق تلك القوانـين على الإنترنـت لأن أمكنتها كلها تعود لملكيات خاصة[105]. لا تنطبق تلك القوانين على ما نقوله في «فيسـبوك» و«تويتر» و«إنسـتغرام» و«ميديوم» وغيرها[106]، ولا على التعليقات التي ندوّنها في مواقع الأخبار، حتى لو كانت مفتوحة للقراءة من قِبَل العموم.

بالعـودة إلى الأيـام الأولى للإنترنت، كانت النقاشـات تجـري في منتديات عامة بواسـطة ما سُـمّي «يوزنِت» (Usenet). مثّلت «يوزنِت» نظاماً غير مركزي لا يتيح

لأي شركة أن تحدّد من يقول ماذا. ومع انتقال منتديات النقاش إلى مواقع الـ«ويب» والمنصّات المملوكة من الشركات، تبخّرت تلك الحريّة.

نحتاج إلى أمكنة على الإنترنت لا تمتلكها أطراف خاصة، بل تكون أمكنة للحديث والحوار والتجمّع والاحتجاج. يمكن أن تكون أمكنة تديرها الحكومة، أو تديرها شركات خاصة تخضع لقوانين معيّنة تجعل من تلك المساحات عموميّة حقاً. وعلى غرار قوانين بث الموجات اللاسلكيّة التي تمنع شركات الاتّصالات من التمييز بين أنواع الموجات المختلفة، من المتصوّر إمكان إيجاد شبكة اتّصال اجتماعي فيها مساحات عامة، ويديرها مُشَغّل عمومي مع منع الشركات من الرقابة والحجب.

أيّاً كانت الحلول، يشكل الجمهور العام والمساحات العموميّة أمراً مهمّاً للمجتمع. يجب أن نعمل بدأب وتقصّد لضمان حضورهم الدائم في الفضاء السبراني.

14

حلول للشركات

في خضـم سـعينا للحدّ مـن الرقابة التي تمارسـها الشركات، من المهـم تذكّر أننا نجنـي فوائد كبرى من تجميع المعلومات واسـتخدامها. إذ يمنحنا تجميع المعلومات فوائد وإمكانات غير مسـبوقة: الحصول على إرشـادات لقيادة السـيارة اسـتناداً إلى معلومات جارية عن حال السـير واختناقاته، قوائم مشـتريات تتذكر ما اشتريناه في المـرّة السـابقـة، إمكان الحصول على تعويضات على المشـتريات حتى لو لم نحتفظ بالفاتـورة، إمكان التأكّد بواسـطة الشـبكة من إطفـاء أنوار المنزل وإغـلاق أبوابه، والتواصـل فوريّـاً مع الأشـخاص في الأمكنة كافة على الكـرة الأرضيّة. هناك مزيد مـن المنافع آتية. تكفي مشـاهدة فيلم خيال علمي للتنبّـه إلى الأعاجيب التي تحصل في عالم مؤتمت كليّاً؛ خصوصاً إذا تأتّت للحواسيب القدرة على فهم ما يفعله الناس والتجـاوب معـه وتذكّره أيضـاً. يمثّل ذلك النـوع من الرقابة مسـتقبلنا الآتي، وهو مملوء بأشياء تجعل حياتنا أفضل وأكثر إمتاعاً.

عـلى نحو مماثـل، هنالك قيمة للوصول الحـرّ إلى التكنولوجيـا. وعلى الرغم من تركيـز معظـم هذا الكتاب على الجانب المظلم مـن التكنولوجيا، يجب علينا تذكّر أن التكنولوجيـا أعطتنا جميعـاً منافع جمّة. إذ تمكننـا التكنولوجيا مـن أداء أعمال معقّدة بسـهولة وسرعـة ودقّـة ما يفيدنا في أشـياء متنوّعـة كتطوير مواد بناء أكثـر ديمومة، العثـور عـلى المعلومات ونشرها، توقّع ظواهـر فيزيائيّة معيّنة بدقـة كبيرة، التواصل

مـع الآخرين مع التحرّر من قيـود الجغرافيا، توثيق الحوادث الجارية، الحصول على طعـام أكثر والعيـش لمدة أطول. لم يكن بمكنتي إنجاز هـذا الكتاب لو لا الإنترنت. لا يعنـي ذلـك أنه كامل بالطبع. وتتوزّع التكنولوجيا بشـكل غير متعادل عبر الكرة الأرضيّـة فيكون هنالك مـن يملكها ومن لا يملكها، لكن- بوجه عام- كلما زادت التكنولوجيا تكون الأشياء أفضل.

إنّ عرقلـة المسـتقبل هـو آخر ما نرغـب في فعله. وببسـاطة، لا نعرف شـيئاً عن المبتكرات الآتية، والمشاكل الإنسانيّة التي تستطيع حلها[1]. نحتاج إلى امتلاك القدرة على التعامل مع التقنيّات الجديدة ومع الأعمال التي تظهر استناداً إلى تلك التقنيّات، بما فيها تقنيّات الرقابة. وتتمثّل المسألة في إيجاد توازن بين الوصول إلى الحـدّ الأقصى مـن الفوائـد المترتبة على تجميع الشركات للمعلومات مـن جهة، وتخفيض الأضرار الناجمة من ذلك إلى الحدّ الأقصى أيضاً.

ثمـة حلول كثيرة تفيـد في الوصول إلى ذلك الهدف. يشـكل «إطار الخصوصيّة» الـذي وضعتـه «منظّمـة التنميـة والتعـاون الاقتصـادي» في 1980، نقطـة انطلاق مناسـبة؛ إذ يرسـم حـدوداً لعمليـات جمع البيانـات وتخزينهـا واسـتخدامها[2]. في 1995، أقـرّ «قانون حمايـة المعلومات» في الاتحاد الأوروبي، بهـدف تنظيم عمليات جمع البيانات الشـخصيّة من قِبَـل الشركات[3]. ولأن الـشركات الأميركيّة تعوّدت عـلى نظـام تشريعـي أقـل صرامـة في بلادهـا، فإنّهـا تبـدي تبرّمهـا بذلـك القانون الأوروبي[4]. ويجري نقاش واسـع حاضراً عـن تحديث ذلك القانون كي يتوافق مع التقنيّات الحديثة[5].

تتعلّـق المقترحـات المقدّمـة في هذا الفصـل بتجميع الشركات الخاصـة للبيانات واسـتخدامها لهـا. أحيانـاً، مـن المحتمـل أن يُطلِـق السـوق بنفسـه بعضـاً من تلك التغييرات، لكن معظمها يتطلّب قوانين تسـهّل تنفيذه. إذاً، يبدو الأمر أشبه بقائمة

ممـا يجب على الحكومة القيام به، ما يعني أنها أيضاً قائمة بما يجب على المواطنون طلبه من الحكومة. ولأن مكوّنات تلك القائمة تمسّ الشركات، فإنها ترد في هذا الفصل.

لتتحمّل الشركات مسؤوليّة اختراقات الخصوصيّة

يشكّل تحميـل الشركات مسـؤوليّة اختراقـات البيانات إحدى الطُرُق الممكنة لتحسين أمن المعلومات المتجمّعة لديها.

باسـتمرار، تعمل الشركات على الموازنة بين التكاليف والأرباح. في هذه الحال، تتمثّـل التكاليـف في تكلفة تجميع البيانات وتخزينها، ومـا يتكلفه الاختراق وانعدام الأمـان، وقيمـة المعلومـات المتجمّعـة. وحـاضراً، لا يتكلّف انعـدام الأمان الشيء الكثير. إذا نحيّنا جانباً تكلفة الحفنة من الاختراقات العموميّة- على غرار ما حدث مـع شركـة «تارغِت»(*)، تجد الـشركات أنه من الأرخص إنفـاق أموال على حملات دعايـة تروّج لجودة الأمن لديهـا، وتوهين الحملات التي تثـور عرضيّاً في الصحافة مثبتة بطلان تلك المزاعم، وكذلك الحال بالنسـبة للقضايا القانونيّة التي تحمل دلالة مماثلة؛ كما أنها لا تصلح الأمور إلا عندما تصل إلى مستوى العلانية.

"إطـار الخصوصـيّة"- "منظّمـة التنميـة والتعـاون الاقتصـادي" (1980)[6]

مبـدأ تنظيـم جمع المعلومات. يجب رسـم حـدود لعملية تجميـع البيانات الشـخصيّة، كـما يجب الحصول على تلـك المعلومات بطـرق قانونيّة وعادلة، إضافة إلى إعلام المعني بها وموافقته، عندما يكون ذلك ملائماً.

مبـدأ نوعيّة البيانات. يجـب أن تتوافق البيانات الشـخصيّة مع الأهداف التي تستعمل من أجلها، ويجب أن تكون دقيقة وكاملة ومحدّثة، ضمن المدى الضروري لأهداف استعمالها.

(*) راجع الفصل 3.

مبدأ تعيين الغاية. يجب تعيين الهدف من جمع المعلومات الشخصيّة ضمن زمن لا يتأخر عن وقت تجميعها، مع مراعاة أن يجري استخدامها لاحقاً بما يتوافق مع تحقيق هذه الغايات أو غايات أخرى لا تكون متعارضة معها، ووفق ما يجري النص عليه في كل حال تشهد تغييراً في الغاية من استعمال تلك البيانات.

مبدأ تنظيم الاستخدام. يجب عدم الإفصاح عن البيانات الشخصيّة، أو جعلها متوافرة أو استعمالها بأي طريقة سوى تلك التي جرى تعيينها في الفقرة 9، ما عدا: أ) وجود موافقة من صاحبها؛ ب) بموجب سلطة القانون.

مبدأ ضمانات الأمن. يجب حماية المعلومات الشخصيّة بضمانات أمنيّة مناسبة تحميها من مخاطر تشمل الضياع والنفاذ غير المشروع والتدمير والتعديل أو الانكشاف.

مبدأ الشفافيّة. يجب الالتزام بسياسة الشفافيّة العامة بصدد التطوّرات والممارسات والسياسات المتعلّقة بالبيانات الشخصيّة. يجب أن تكون السُبُل متوافرة دوماً للتأكّد من وجود البيانات الشخصيّة وطبيعتها، والغاية الرئيسة من استخدامها، إضافة إلى تحديد هويّة المشرف على تلك البيانات ومكان إقامته.

مبدأ المشاركة الفرديّة. يجب أن ينال الأفراد الحق في: أ) الحصول من المشرف على البيانات أو من في حكمه، على تأكيد لحيازته/ عدم حيازته بيانات تتعلّق بهم؛ ب) أن يجري إبلاغهم بالبيانات المتّصلة بهم. 1 - ضمن مدّة معقولة 2 - بسعر لا يكون باهظاً، إن وُجِد أصلاً 3 - بطريقة معقولة 4 - بشكل يكون مفهوماً لديهم؛ ت) الحصول على أسباب في حال عدم قبول تقدّمهم بطلب تحت البندين أ وب، مع إمكان أن يتحدّوا ذلك المنع؛

ج) أن يتحدّوا معلومات منسوبة إليهم، وفي حال نجاحهم بذلك، يفترض أن تمحى تلك المعلومات أو تعدّل أو تستكمل أو تصحّح.

مبدأ الموثوقيّة. يفترض بالمشرف على البيانات أن يكون موضع ثقة بالنسبة للاستجابة إلى الإجراءات التي تتعلّق بتفعيل المبادئ المنصوص عليها أعلاه.

يرجع السبب في ذلك إلى أن تكلفة اختراقات الخصوصيّة تقع على كاهل الجمهور الذي تنكشف بياناته. في علم الاقتصاد، يسمّى ذلك "خرجانيّة" بمعنى أن تأثير القرار لا يقع على عاتق متّخذه. وتحدّ "الخرجانيّات" من حماسة الشركات لتحسين أمنها.

ربما تتوقّع أنّ يكون ردّ فعل الجمهور على ذلك هو تفضيل الخدمات المأمونة على غيرها؛ فبالنتيجة يتّخذ الجميع قرارات شرائهم بناءً لنموذج السوق نفسه. لكن، تذكّر أنّ ذلك ليس متاحاً عموماً. في بعض الأحيان، تحدّ بعض الاحتكارات في البرمجيات ما يتوافر من خيارات للجمهور. في حالات أخرى، يبرز تأثير "تناسب القفل مع المفتاح" الذي تتعمّده بعض الشركات التجاريّة البارزة في التكامل بين تركيبة الملفات، والبنية التحتيّة المتاحة، ومتطلّبات التوافق؛ أو بواسطة تقديم البرامج على هيئة خدمات؛ ما يصعب عملية الانتقال من خيار إلى آخر. في حالات كثيرة، لا نعرف من يجمع بياناتنا، كما ورد في النقاش عن الرقابة الخفيّة في الفصل 2. في الحالات جميعها، يصعب على الشُراة تقييم مدى مأمونيّة الخدمات. ولا يتعلّق الأمر بالشُراة غير التقنيّين، فحتى أنا لا أستطيع أن أفيدك عمّن تكل إليه خصوصيّتك بثقة من بين مقدّمي الخدمات المختلفة.

يتغيّر ذلك مع تحميل الشركات المسؤولية القانونيّة للاختراقات. ومع رفع تكلفة اختراق الخصوصيّة[7]، نستطيع دفع الشركات للقبول بتكاليف «الخرجانيّة»، وإجبارهم على بذل جهد أكبر لحماية خصوصيّة أولئك الذين تجمّعت بياناتهم لديها.

في الولايـات المتّحـدة، يحصل ذلـك فعليّاً مع بيانات الرعايـة الصحيّة؛ لأن اختراق خصوصيّة البيانات فيها يترتب عليه غرامات باهظة[8].

وكذلـك شرع أمـر مماثـل في الحـدوث أميركيّـاً، في بيانـات المتاجر أيضـاً[9]. إذ تواجِـه «تارغِت» حاضراً دعاوى قانونيّة ترتبت على اختراق البيانات لديها في العام 2013 [10]. في حالات أخرى، جرت مقاضاة بنوك بسبب عدم وجود أمن مناسب لبيانات زبائنهم[11].

ربما تمثّلت إحدى الطُرُق التي تساعد على ذلك، في الطلب من الشركات بأن تبلغ المستخدمين عن *كل* المعلومات التي تملكها بشأن البيانات التي تعرّضت للضرر.

ربـما تكـون تلك الحـالات معقّدة، إذ تتـضرر مجموعة من الـشركات معاً في كل حادثـة، ما يصعّب التوزيع المتناسـب للمسـؤوليّات عليها[12]. وتتلـكأ المحاكم في تحديد قيمة معيّنة للخصوصيّة؛ لأن الناس تخلّوا طواعية عنها أصلاً مقابل الحصول عـلى القليـل. ولأنه من الصعوبـة الربط بين الأضرار الناجمة مـن فقدان الخصوصيّة مـن جهة، والأفعال التي أدّت إلى تلـك الأضرار من الجهة الثانية، كان من الصعب كسب تلك الدعاوى.

هناك طريقة أفضل لمقاربة الأمر عينه: جعل القضية حدوث اختراق للخصوصيّة وليس ما ترتب على ذلك من أضرار. يجب إجبار الشركات على الانصياع إلى قوانين كـ «قانـون الممارسـات العادلة في المعلومات» (1973)[13] وما يشـبهه من قوانين لم تعد ملزمة حاضراً؛ وعندها يصبح الاعتداء هو الفشل في الالتزام بالقوانين.

"قانون الممارسات العادلة في المعلومات" (الولايات المتّحدة- 1973)

يستند "قانون الممارسات العادلة في المعلومات" إلى 5 مبادئ:

1 - ألا يكون وجود نُظُم سجلات المعلومات الشخصيّة بحد ذاته سريّاً.

2 - إيجاد طريقة كي يعرف المرء ما هي المعلومات المسجّلة عنه، وكيف تستخدم.

3 - إيجاد طريقة يتمكن فيها المرء من منع وضع معلومات عنه جرى جمعها لغاية محدّدة في خدمة غايات أخرى إلا بموافقته.

4 - إيجاد طريقة تمكّن المرء من تعديل أو تصحيح سجل معلومات عنه، عندما تكون قابلة لأن تكون معروفة.

5 - على كل منظّمة تصنع أو تصون أو تستعمل أو تنشر سجلات فيها معلومات شخصيّة قابلة لأن تكون معروفة، أن تضمن مصداقية البيانات بالنسبة للغاية من استعمالها، كما يجب عليها اتّخاذ احتياطات كافية لمنع سوء استعمال البيانات.

هنالك وضعيّة موازية تتمثل في قوانين "وكالة حماية البيئة" (Environment Protection Agency) بشأن ملوّثات البيئة[14]. فعندما تتخطى الملوّثات نسباً بعينها، تضحي عرضة للغرامات. لا حاجة لانتظار ظهور ارتفاع مفاجئ في حالات السرطان. تكون المسألة مفهومة، والقوانين مجهّزة، ويكون على الشركات أن تقرّر بشأن بناء مصانع تعمل على الفحم أو الألواح الشمسيّة؛ وتكون العقوبات بالانتظار إذا فشلت الشركات في الانصياع إلى ما يمثّل أفضل الممارسات بصورة أساسيّة. يجب أن نمضي في ذلك الطريق.

بالتأكيد، يؤول جعل النُظُم أكثر أماناً إلى زيادة التكاليف، وستسعى الشركات إلى إلقاء ذلك العبء على كاهل المستخدم بزيادة الأسعار، إذا تمكّنت من ذلك. لكن، بات المستخدمون يدفعون فعلياً تكلفة النُظُم غير الآمنة بالتكاليف المباشرة وغير المباشرة للاختراقات. تحميل الشركات المسؤوليّة القانونيّة عن الاختراقات، ينقل تلك التكلفة إليها ويؤدّي تالياً إلى دفعها لتحسين أمنها[15]. أفضل مصطلح

يعطيه علم الاقتصاد على ذلك هو «المتجنّب بالكلفة الأقل»[16]، بمعنى أنه من المجدي اقتصادياً إلقاء المسؤولية على الطرف الذي يمتلك البيانات؛ لأنه في الوضع الأفضل لتقليص المخاطر إلى أقصى الحدود. فكّر في الأمر: ماذا تستطيع أن تفعل كي تجبر «فيسبوك» على تقديم حماية أفضل لبياناتك الشخصيّة؟ ليس كثيراً[17]. تفيد النظرية الاقتصادية أنّ ذلك يمثّل سبباً لتحميل الشركة تكاليف ممارساتها السيّئة في الأمن.

قوانين لاستعمال البيانات

خلافاً للحال في الاتحاد الأوروبي، لا تعتبر الولايات المتّحدة أن المعلومات الشخصيّة هي ملك لك، بل تملكها الجهة التي تجمعها. تحمي القوانين أنواعاً معيّنة من المعلومات الشخصيّة- كالبيانات المالية، ومعلومات الرعاية الصحيّة، وبيانات الطلبة، وسجلات استئجار أشرطة الفيديو- لكن الأميركيّين يفتقرون إلى قوانين عن الحماية الواسعة للخصوصيّة على غرار الحال في البلدان الأوروبيّة. في المقابل، تمثّل الحمايات القانونيّة الواسعة الحل الوحيد فعليّاً؛ مع ملاحظة أن ترك الحبل على غاربه للسوق في تحديد ذلك سوف يؤدي إلى مزيد من الرقابة الواسعة العدوانيّة.

خذ هذا المثل: تعمل شركة «داتايوم» (Dataium) مع الأفراد أثناء شرائهم سيّارات بواسطة الشبكة. وتترصد زيارتك للمواقع الشبكيّة لمختلف صُنّاع السيّارات، فتلاحظ نوع السيارة التي تبحث عنها، الخيارات التي تنقر عليها لتعرف مزيداً من المعلومات عنها، الخيارات الماليّة التي تفتش عنها، وكم من الوقت تقضيه في مطالعة صفحات بعينها. يدفع المتعاملون أموالاً مقابل تلك المعلومات عنك، إذ إنّها لا تتصل بالسيّارات التي يبيعونها، بل السيّارات التي صنعتها شركات أخرى ولفتت اهتمامك كثيراً[18]. ويدفعون مقابل تلك المعلومات لأنك إذا قصدت معارضهم، يصبحون أكثر قدرة على بيع سيارة لك بما يضمن ربحاً أكثر لهم.

عنـد هـذه النقطـة، فكّـر في الاقتصاديّات. بإمـكان تلك المعلومـات أن تكلّفك (بأدنى تقدير) قرابة 300 دولار من السعر النهائي الذي تدفعه لشراء سيارتك.

يعني ذلك أن حمايتك من ممارسـات «داتايوم» لا تسـاوي أكثر من 300 دولار. لكن، هنالك 12 مليون سيارة تباع سنويّاً في الولايات المتّحدة. حتى لو افترضت أن «داتايـوم» تملك بيانات تتصل بـــ2 في المئة منهم، فإن ذلك يعني أن التكتيكات التي تتبعها تلك الشركة تساوي 100 مليون دولار سنويّاً.

يشكّل ذلك التفاوت السبب في فشل الحلول الآتية من السوق. إنها مسألة عمل جماعي. إذاً، عملنا المشـترك في حماية أنفسـنا من ممارسـات «داتايوم» يسـاوي 100 مليـون دولار، لكننـا لا ننسـق أعمالنا معـاً. وتربط «داتايوم» بين وكلاء السـيّارات بصورة طبيعيّة، لكن الوسيلة الوحيدة للربط بيننا كمستهلكين هو الفعل السياسي.

إنّ نقـاط الاسـتعمال هـي مـكان منطقي لفرض قوانـين تنظيميّـة؛ لأن كثيراً من البيانـات التـي تُجمَع عنّا يجري تحصيلها عندما نكون راغبين في ذلك. ونحتجّ عندما تسـتعمل البيانات بطرق لم نكن نقصدها: عندما تخزّن وتُشـارك وتُباع وتُنسّـق، ثم تسـتخدم للتلاعـب بنـا بطـرق خفيّة. يعنـي ذلك وجـود حاجة لقيود عـلى الطرق الممكنـة في اسـتخدام بياناتنا، خصوصاً تقييد تلك الطُرُق التي تغاير الأهداف التي جمعت تلك البيانات لأجلها.

تثـور مسـائل أخرى عندمـا تعامـل الـشركات جـداول خوارزميّاتهـا بوصفها أسراراً تجاريّـة. هنـاك مثلان على ذلـك هما: جدول خوارزميّـة «بايج رانك» (Page Rank) في «غوغـل» الـذي يحدّد نتائج البحـث التي تعرض عليك، ونُظُم تسـجيل بيانـات بطاقات الائتمان. تملك الشركات هاجسـاً شرعيّاً بالسريّة. وتخشـى وصول المنافسـين إلى خوارزميّاتهـا وبياناتهـا (مـع قدرتهم على نسـخها)، قدر خشـيتها من وصول الجمهور إليها وانكشـاف طرق عملها أمامه. وشـخصيّاً، أرى أن الشـفافيّة تتقـدّم على الملكيّـات التجاريّة في الأحوال التي تطـاول الخوارزميات فيها الجمهور

بتأثيراتهـا[19]. مـن المسـتطاع جعل المزيد مـن الخوارزميـات علنيّة- بـل تصميمها لتكون قابلة للعلانية- بالمقارنة مع ما يحصل حاضراً[20]. لسـنوات طويلة، فرضت الصراحـة في القروض وقوانين العدل فيها أن تكون الخوارزميات التي تسـتخدمها المؤسّسـات الماليّـة، قابلـة للشرح والمسـاءلة القانونيّـة. يجب مدّ أطر تلك الشـفافيّة المفروضة إلى مساحات أخرى تمارِس فيها الخوارزميات سلطتها على الناس؛ بمعنى جعلهـا مفتوحـة. وفي المقابل، هنالك طُرُق في تدقيـق الخوارزميات تضمن عدالتها مع الحيلولة دون انكشافها للعلن[21].

تميل الشركات لأن تكون منطقية في تقييم المخاطر، وستتقيّد بالقوانين. إنّ المفتاح الحقيقي لنجاح ذلك الأمر هو الإشراف والموثوقيّة. ليسـت تلك أشـياء اسـتثنائيّة، فهنالـك قوانـين كثـيرة تنظّـم صناعـات أميركيّة عـدّة؛ لأننا نعـرف أن مـا يفعلونه هـو مهـم وخطر في آن معـاً. وليس من فارق بـين ذلك وبين المعلومات الشـخصيّة وخوارزميات تحليلها.

يجب إرسـاء آليّة للتدقيق تضمن التزام الشركات بالقوانين، وتعاقبها إن لم تفعل ذلك.

يبـدو ذلك كلـه منطقياً من الناحية النظريّة، لكن تنفيذه صعب. الحال أن آخر ما نرغب به هو أن تبدأ الحكومة بالقول: «يمكنكم أن تفعلوا ذلك حصراً، لا سـواه»، بالنسبة لبياناتنا ومعلوماتنا. إذ تتكفّل القوانين التنظيميّة المستندة إلى الأذن الحكومي المُسـبَق، بخنق التغيـير والابتكار التقني. إننا نسـعى إلى قوانين تنظيميّة مسـتندة إلى الحقوق أساساً، فيكون شعارها: «تستطيع فعل ما تشاء، طالما أنه ليس محظوراً».

تنظيم جمع المعلومات أيضاً

لا يكفي تنظيم اسـتخدام البيانات. إذ يجب تنظيم الخصوصيّة في مسارات كثيرة تشمل جمع البيانات وتخزينها واستعمالها، وكذلك الخلافات بصددها. ويُظهِر «إطار

الخصوصيّة» في «منظّمة التنمية والتعاون الاقتصادي» (1980) تلك الأشياء بطريقة حسنة، وهي أساسيّة كلها. ولسنوات طويلة، بذلت الشركات الأميركيّة جهوداً منسّقة لإقناع العالم بعدم الحاجة إلى قوانين لتنظيم جمع المعلومات، والاكتفاء بقوانين استخدامها[22]. تسعى الشركات إلى التخلّص من القيود على جمع البيانات؛ لأنها تعلم أن القيود على استعمال البيانات ستكون صعبة التحديد وضيّقة المدى، وأنها [الشركات] تستطيع توسيعها تدريجيّاً ما أن تصبح بياناتنا في أيديها. (ثمة حجة رائجة ضد كل قانون لتنظيم استخدام البيانات تتمثّل في وصمه بأنّه شكل من الرقابة). وتعلم الشركات أنه بمجرد وضع قوانين لتنظيم جمع البيانات، يصبح من الصعب تغييرها. ولكن، على غرار الرقابة الحكوميّة العامة، يلحق الضرر بالخصوصيّة من محض تجميع البيانات، وليس حصراً من استعمالها[23]. أذكّر بالنقاش عن الرقابة بالخوارزميات في الفصل 10. سوف ينجم عن عدم تنظيم جمع المعلومات إلى تجميع واسع لها، ومشاركة مفرطة للبيانات مع الحكومة، مع تآكل بطيء للقيود الضروريّة المحدّدة بدقة على استخدام البيانات.

يجدر بنا القتال ضد تلك الحملة. ليست القيود على جمع المعلومات أمراً مستحدثاً. إذ لا يطلب من الموظفين المعنيين أن يسألوا المتقدّمات إلى وظيفة ما عما إذا كُنّ حوامل. لا يسمح لاستمارات طلب القروض البنكيّة أن تتضمن سؤالاً عن عرق المتقدّم بالطلب. مثّلت التسوية القديمة بشأن عدم طلب الإفصاح عن الهويّة الجنسيّة بالنسبة للجنود مثليّي الجنس في الجيش الأميركي، وهي التي لخّصها شعار «لا تسأل، لا تُخبر»، قيداً على جمع المعلومات. وهناك قيود على ما يستطيع «المكتب الأميركي للإحصاء» أن يسأل الناس عنه.

لن يكون من السهل نقل تلك الأمور إلى عالم يتحكّم فيه الكومبيوتر بكل ما نفعله، لكن يجب أن نبدأ بالنقاش عن المعلومات التي يجب عدم السؤال عنها أبداً. ثمة أمكنة واضحة للانطلاق منها. يجب أن يكون ما نقرؤه على الشبكة الإلكترونيّة بمثل خصوصيّة ما نقرؤه ورقيّاً. ويعني ذلك ضرورة وضع حدّ قانوني للسجلات

عـن الصفحات الشـبكيّة التي قرأناهـا، والوصلات الإلكترونيّة التـي نقرنا عليها، ونتائـج عمليـات البحـث التـي أجريناهـا عـلى الإنترنـت. ينطبق الأمر نفسـه على تحرّكاتنـا، بمعنـى ضرورة التخلّص من حال يكون فيه اقتنـاء الخلوي رديفاً للوقوع في آسـار رقابة مسـتمرة. يجب التوقّف عن الرصد المسـتمر لعلاقاتنا، بمعنى مع من نلتقي في الشـارع ومن نتحدث إليهم. لربما سُـمِح لشركات بأن تسـتخدم بعضاً من بياناتنـا فوريّاً، شريطة أن تتخلّص منها. ولربما سُـمِح لـشركات بالاحتفاظ ببياناتنا لبعض الوقت، شريطة ألا يطول.

هنـاك فكـرة جذّابة طرحها البروفسـور ميخائيل فرومكين، وهو أسـتاذ في كلية القانـون بجامعة ميامي[24]. تتمثّل الفكـرة في إلزام الوكالات الحكوميّة والشركات الخاصة، لدن انخراطها في عمليات واسعة لجمع المعلومات، بأن توقّع «تعهّداً بشأن تأثـير الخصوصيّـة» يكون على شـاكلة «تقارير الأثر البيئـي». إذ يفيد ذلك في إعلام الجمهور عما يُجمَع من بيانات مع تبيان سبب جمعها. وسوف يحثّ ذلك صُنّاع القرار عـلى التفكير في الخصوصيّة في مرحلة مبكّرة من تطوير مشـاريعهم، مع التماس آراء الناس بصددها.

يصلح خيار الدخول كنقطة انطلاق. وبشكل أساسي، هناك طريقتان للحصول عـلى موافقة. يعني خيار الدخول اشـتراط الحصول على موافقتك الصريحة قبل جمع بياناتـك واسـتخدامها. يعني خيـار الخروج نقيض ذلـك تماماً، بمعنـى أن بياناتك سـتُجمَع إلا إذا اخترت الاحتجاج صراحة على ذلك. تميل شركات كـ «فيسـبوك» إلى تبنـي خيار الخـروج؛ لأنّها [الـشركات] تسـتطيع جعل العثور عـلى ذلك الخيار صعباً، كما أنها تعلم أن معظم الناس لا يبالون بالأمر. يبدو خيار الدخول أشد عدلاً بكثـير، كـما يجب عدم جعل استخدام الخدمة مشروطـاً بالموافقة على جمـع البيانات والمعلومات.

حتى الآن، لا جانب مظلم لجمع البيانات وتخزينها كلها. ومع تقييد ما تستطيع الشركات جمعه من المعلومات وما تستطيع فعله بها، ومع جعل الشركات مسؤولة عن البيانات المتجمّعة لديها، ومع إرغامها على النزاهة التامة مع الجمهور بشأن ما تجمعه حقاً وكيف تتصرف به؛ نصل إلى وضع نؤثّر فيه في الشركات كي يقتصر ما تجمعه وتخزّنه من بيانات عنّا، على ما تعرف الشركات أن له قيمة حقاً.

يجب على الكونغرس أن ينخرط في عمل دؤوب لتحديث قوانين الخصوصيّة في الولايات المتّحدة، والتوقّف عن إعطاء الذرائع لتقاعسه. تستطيع المحاكم أيضاً أن تؤدّي دوراً مهماً في ضمان خصوصيّة المستهلك، بتفعيل القوانين السارية بشأن الخصوصيّة. تحوز بعض الوكالات التشريعيّة، كـ «اللجنة الفيدراليّة للتجارة» و«اللجنة الفيدراليّة للاتّصالات»، بعض السلطة في حماية خصوصيّة المستهلك في مجالات معيّنة[25]. في المقابل، تحتاج الولايات المتّحدة حاضراً إلى وجود وكالة مستقلّة لحماية المعلومات، أسوة بما هو حاصل في بلدان كثيرة[26]. ونحتاج إلى ما هو أفضل من المسارعة إلى سدّ المشكلات عندما ينتج عنها ضرر كافٍ. إنّها تحدّيات كبيرة ومعقّدة، وتحتاج إلى وجود وكالة تملك خبرة ومصادر كافية للتأثير فيها بشكل مجدٍ.

إنجاز العمل ببيانات أقل

إلى حدّ كبير تماماً، تستطيع المؤسّسات إنجاز أعمالها مع تجميع بيانات أقل كثيراً مما تفعله الآن، وتخزينها لفترات أقصر أيضاً. المفتاح اللازم لذلك هو أن تفهم [الشركات] كمية البيانات التي تحتاجها، وتحدّد الغاية منها.

مثلاً، تعمل نُظُم كثيرة على تجميع هويّات المستخدمين دون حاجتها إلى تلك المعلومات. وغالباً، يكون التفويض هو كل ما تسعى إليه. لا يحتاج موقع للتواصل الاجتماعي إلى معرفة هويّتك الحقيقيّة. وكذلك الحال بالنسبة الشركة التي تعمل على تخزين البيانات في «سُحُب المعلومات».

ثمة أنواع من تحليل البيانات تتطلّب الحصول على بيانات عن أشخاص كثيرين، لكن ليس كل شخص. لننظر إلى تجربة شركة «وايز» (Waze). إنّها تستخدم معلومات الرقابة لتتبع أوضاع حركة السير، لكنها لا تحتاج إلى معلومات عن كل شخص كي تنجز عملها. إذا وضعت تحت الرقابة عدداً من السيّارات يكفي لتغطية الشوارع الرئيسة، فسيكون ذلك كافياً. وتعتمد مجموعة من محلات البيع بالتجزئة على الرقابة الشاملة لقياس فعالية إعلاناتها، واستنتاج أنماط الشراء عند الجمهور وغيرها. كرّة أخرى، لا تحتاج تلك المحلات إلى بيانات الناس كلها. إذ تكفي عيّنة إحصائيّة جيّدة الدلالة لتلك التطبيقات، وهو أمر كان رائجاً عندما كان جمع المعلومات مكلفاً.

هنالك تطبيقات تميل لتجميع بيانات عن الجميع كي تزيد فعاليّتها، ببساطة[27]. لكن، من المؤكّد أن «غوغل» سيعمل جيّداً إذا امتلك بيانات عن نصف جمهور مستخدميه، لكنها ستكون تجارة أقل ربحاً. يبقى أن ثمة تطبيقات تحتاج البيانات كلها. إذا كنت شركة للخلوي تسعى إلى إيصال المكالمات الهاتفيّة، فستحتاج إلى معرفة موقع كل مستخدم، وإلا سينهار النظام بأكمله.

ثمة تفاوتات بين الشركات في مدة تخزين البيانات. تحتاج «وايز» والشركة التي تقدّم لك خدمات الخلوي إلى معرفة موقعك باستمرار، في الوقت الحي. يحتاج المعلنون إلى بعض البيانات المتسلسلة زمنيّاً، لكن المعلومات الأكثر جدّة تكون أشد أهمية لهم. من الناحية الثانية، هناك بيانات فائقة القيمة للبحوث. ومثلاً، تضخ شركة «تويتر» بياناتها إلى «مكتبة الكونغرس»[28].

نحتاج إلى قوانين ترغم الشركات على جمع الحدّ الأدنى اللازم من البيانات، والاحتفاظ بها لأقل زمن لازم، مع حفظها بطريقة أكثر أمناً مما تفعله [الشركات] الآن. وكما يبدو متوقّعاً، تملك اللغة الألمانية كلمة واحدة لوصف ذلك كله هي «داتنشبارشزامكايت» (Datensparsamkeit)، وهي تعني «اقتصاد البيانات»[29].

إعطاء الناس الحق في بياناتها

الولايـات المتّحـدة هـي البلـد الغـربي الوحيـد الـذي لا يملـك قوانـين لحمايـة البيانـات[30]. تملـك أميركا حمايات لبعـض أنواع المعلومات، لكنها تشـمل حقولاً معزولـة[31]. بصـورة عامـة، فإنّ حقـوق الأميركيّين في بياناتهم تتسـم بالتشـوش. و«يتذكّر» محرّك البحث «غوغل» معلومات عن حياتي، نسيتها أنا منذ زمن طويل[32]. يرجع ذلك لامتلاك «غوغل» سجلاً عن عمليات البحث التي أجريتها طيلة حياتي، لكني لا أملك نفاذاً إليها كي أنعش ذاكرتي. تزعم شركة «ميدترونِك» أن المعلومات الموجودة في أجهزتها لإنعاش القلب بالصدمة الكهربائيّة، هي ملكيّة تجاريّة لها، ولا تتيـح للمرضى الذين جـاءت من قلوبهم تلك البيانات الحـق في الوصول إليها[33]. في الاتحاد الأوروبي، يملك الناس الحق في معرفة المعلومات والبيانات المتعلّقة بهم. ولذا، اسـتطاع الشـاب ماكس شريمز إرغام شركة «فيسـبوك» على إعطائه البيانات المتعلقة به لديها كافة(*). لا يتمتع المواطنون الأميركيّون بذلك الحق.

لا يسـهل تصـوّر الطريقة التي يجـب تفعيل تلك الحقوق بها. مثـلاً، يمكن إيراد قائمة عن أنواع البيانات التي ننتجها بأنفسنا على شبكات الـ «سوشال ميديا»[34]:

* بيانـات الخدمة: إنهـا البيانات التي تعطيها للشـبكة الاجتماعية كي تحصل عليها. ووفقاً لكل موقع، يحتمل أن تشـمل تلك البيانات اسمك القانوني وعمرك ورقم بطاقتك الائتمانيّة.
* بيانـات مُعلَنَـة: هي التدوينـات التي تخطّهـا على صفحتك، بـما فيها مواد المُدوّنـات الإلكترونيّة، والصور وأشرطة الفيديو والرسـائل والتعليقات وغيرها.

(*) راجع الفصل 1 في الكتاب.

* **البيانـات الموثوقـة:** إنّها مـا تكتبه على صفحات الآخرين. وتشـبه أساسـاً البيانـات المعلنة، ويكمن الفارق في أنك لا تحظى بالسـيطرة عليها، بل إن المستخدم الآخر هو الذي يحظى بها.

* **البيانـات العرضيّـة:** هي مـا يكتبه آخرون عنك. ربما كانـت فقرة تتحدث عنك في شيء كتبه شـخص ما، أو ظهورك في صورة التقطها شـخص آخر ووضعهـا عـلى الإنترنـت. لا يقتصر الأمر عـلى أنك لا تسـيطر على تلك البيانات، بل إنك لم تصنعها أصلاً.

* **البيانات السلوكيّة:** إنّها البيانات التي يجمعها الموقع عن عاداتك، بمراقبته ما تفعله والأشخاص الذين تتعامل معهم.

* **بيانات مشتقّة:** هي معلومات عنك تُستخلَص من البيانات الأخرى كافة. مثـلاً، إذا عـرّف 80 ٪ مـن أصدقائك أنفسـهم بوصفهـم مثليي الجنس، فالأرجح أنّك مثليّ الجنس أيضاً.

ما هي الحقوق التي تملكها في أنواع تلك البيانات كلها؟ في الوضع الحاضر، كل تلـك البيانات موضوعة عـلى الطاولة. هناك أنواع من البيانات تحتفظ بخصوصيّتها دومـاً، بعضهـا يمكن جعله خصوصيّـاً، وبعضها يبقى عموميّاً دوماً. من المسـتطاع تعديل بعض البيانات أو حذفها- شـخصيّاً، أعرف موقعاً يسـمح بحذف البيانات الموثوقة بصورة نهائيّة خلال 24 ساعة- ويستعصي بعضها على ذلك. يمكن الاطلاع على بعض البيانات، ولا يسمح بذلك بالنسبة لبيانات أخرى. لا قوانين في الولايات المتّحـدة عـن البيانات، ويجب على مـن يملكون البيانات أن يقرّروا بأنفسـهم، وهم بالتأكيد يحظون بنفاذ كامل لها.

تقـدّم لـك بعـض المنصّـات إمكانـات مختلفـة في تقييـد مـن يطلع عـلى بيانات اتّصالاتـك. ووصـولاً إلى العام 2011، كان «فيسـبوك» يتيح لـك إمكان تقييد من يطلعـون عـلى تدويناتك، بمعنى اقتصار ذلـك على أصدقائـك أو إتاحتها للعموم. وعنـد تلـك النقطـة مـن الزمن، كان «فيسـبوك» يسـمح لـك بالتحكّـم بمجموعة

أصدقائـك، وبـأن تطلع بعضـاً منهم على تدويناتـك، وليس كلّهم بالـضرورة[35]. تنقسـم التغريـدات إلى مـا يوجّه إلى أشـخاص بعينهم، وما يعلن عـلى الملأ[36]. من المتـاح جعل تدوينات «إنسـتغرام» سريّة، أو مقروؤة من أشـخاص بعينهم، أو معلنة للعموم[37]. وتمنح صفحات موقع «بينترست» إمكان جعلها معلنة أو سريّة[38].

مـن المهـم وضع معايير لتلك الأمور. في العـام 2012، أصدر «البيت الأبيض» مـا يعرف باسـم «وثيقة حقـوق الخصوصيّة للمسـتهلك». في 2014، أوصت لجنة مراجعة رئاسـيّة عن الخصوصيّة و«البيانات الضخمة»، بجعل تلك الوثيقة أساسـاً في التشريع[39]. أوافق على ذلك تماماً.

من السهل المضي بعيداً في ذلك المفهوم. يقترح يارون لانير، عالم كومبيوتر وناقد للتقنيّـة، خطّـة تقـضي بأن نحصل تلقائيّـاً على جُعالَة مِـنْ كُل مَنْ يَسـتخدم بياناتنا، سـواء أكان محرّك بحث يسـتعملها لإيصال إعلانات إلينا أم تطبيقاً رقمياً يستعملها لتحديـد درجـة اختناق المرور[40]. بالطبع، سـتكون جُعالَة ميكروسـكوبيّة، أو ربما نانويّة؛ لكنها ربما تراكمت لتصل إلى حفنة من الدولارات. يتّسـم تنفيذ تلك الخطة بالتعقيـد الفائـق، وبالنتيجة يحتـاج التنفيذ إلى رقابة مسـتمرة حتى لو أنه يسـعى إلى تحويل الرقابة إلى مصدر مالي لكل شـخص. تتمثّل المسـألة الأساسيّة في تبني مفهوم الخصوصيّة بوصفها شـيئاً قابلاً للتجارة بتلـك الطريقة. لكن الخصوصيّة يلزمها أن تكون حقاً أساسيّاً، وليس ملكيّة تجاريّة.

"وثيقة حقوق الخصوصـيّة للمسـتهلك" - الولايـات المتّحدة (2012)[41]

التحكّم الفردي. يحق للمستهلكين ممارسة التحكّم بالبيانات الشخصيّة كافة التي تجمعها الشركات منهم، وكذلك طُرُق استعمال تلك البيانات.

الشـفافيّة. يحقّ للمسـتهلكين الحصول على معلومات بخصوص ممارسـات الأمن والخصوصيّة تكون سهلة الفهم والوصول.

احترام السياق. يحقّ للمستهلكين توقّع أن تجمع الشركات بياناتهم الشخصيّة وتستعملها وتكشفها بطُرُق تتناسب مع السياق الذي أعطى فيه المستهلكون تلك البيانات.

النفاذ والدقّة. يحقّ للمستهلكين الوصول إلى بياناتهم الشخصيّة وتصحيحها في الملفات قيد الاستخدام، بطريقة تتناسب مع حساسيّة البيانات والمخاطر المتنوّعة التي قد تنجم إذا لم تكن البيانات صحيحة.

الموثوقيّة. يحقّ للمستهلكين أن تكون بياناتهم الشخصيّة بيد شركات تتقيّد بإجراءات مناسبة لضمان توافقها مع «وثيقة حقوق الخصوصيّة للمستهلك».

يجب أن نمتلك الحق في الحذف. يجب أن نكون قادرين على القول لكل شركة أوكلنا إليها بياناتنا: "نحن نغادرك. نرجو حذف البيانات المتعلقة بنا كافة". يجب أن تكون قادراً على القول لسماسرة المعلومات والبيانات: "لست منتجاً بيدك. أنا لم أعطك أبداً الإذن بجمع معلومات عني وبيعها للآخرين. أريد إخراج بياناتي من قاعدة بياناتك". يحاول الاتّحاد الأوروبي التعامل مع ذلك الأمر: الحق في النسيان[42]. في العام 2014، قضت «محكمة العدل الأوروبيّة» بأنه في بعض الأحيان، يجب على محرّكات البحث أن تحذف معلومات عن أفراد من نتائج عمليات البحث فيها[43]. أدّى ذلك إلى تدفّق سيول من الناس على «غوغل» طالبين حذف نتائج بحث لا تعبّر عنهم بدقة؛ وشملت صفوف هؤلاء سياسيّين وأطباء والميّالين جنسياً إلى الأطفال[44]. من المستطاع إثارة نقاش عن خصوصيّات تلك الحال، وإذا كانت المحكمة توصّلت إلى التوازن الصحيح، لكن يبقى أن ذلك حق مهم للمواطنين في بياناتهم التي تستفيد الشركات منها[45].

إبراز الخصوصيّة وجمع البيانات

طيلة الوقت، نُبرِز بيانات عن أنفسنا إلى العائلة والأصدقاء والزملاء والمحبّين، بل حتى الغرباء. نتشارك معلومات مع أطبّائنا ومستشارينا الماليّين وأطبائنا النفسيّين.

نتشارك معلومات كثيرة. لكننا نفكر بتلك المشاركة على طريقة المعاملات: أنا أتشارك معك بيانات لأنني أريد أن أطلِعَك على أشياء، أو لأنني أئتمنك على أسراري، أو أنني أتعامل معك بالمثل لأنّك أطلعتني توّاً على شيء ما خصوصي بشأنك.

لقد طوّر الجنس البشري نُظُماً سيكولوجيّة من الأنواع كافة، لاجتياز تلك المفازة من القرارات بشأن الخصوصيّة. وتتميّز تلك النُظُم بأنّها معقّدة بشكل استثنائي، عالية التناغم، وحساسة اجتماعيّاً. تدخل إلى حفلة ما فتعرف فوراً كيف يجب أن تتصرّف. تعرف لمن تتحدث، ما الذي تقوله لمن، من يقترب منك ومن يصغي إليك؛ يستطيع معظمنا اجتياز تلك التجربة بصورة طيبة. ثمة مشكلة في كون التقنية تثبّط تلك القدرة الاجتماعيّة. انقل مشهدية تلك الحفلة إلى «فيسبوك»، يبدأ حدسك في الخوار فجأة. إذ ننسى من يقرأ تدويناتنا. وعلى نحو عرضي، ربما وضعنا شيئاً خصوصيّاً في متناول العلن. لا نفهم كيفيّة ترصد بياناتنا في خلفية الموقع. لا ندرك ما تستطيعه التقنيّات التي نستعملها، وما الذي تعجز عنه.

وإلى حدّ كبير، يرجع ذلك إلى عدم إبراز درجة الخصوصيّة على شبكة الإنترنت. يتواهن الحدس عندما تتوارى أفكار الخصوصيّة في خلفيّة المشهد. عندما لا نقدر على فهم الناس، يحيق بنا الفشل. إذ لا نفكّر بشيء من قبيل «هناك شركة تسعى إلى الربح تسجّل كل شيء وتسعى إلى تحويل ذلك إلى إعلانات». لا نفكر بأنّ «الولايات المتّحدة وربما حكومات أخرى تسجّل كل ما أقوله، وتبحث عن الإرهابيّين أو المجرمين أو مهرّبي المخدّرات أو كل شخص سيئ اختارته هذا الشهر». ليس ذلك ما يبدو واضحاً في مشهديّة الإنترنت. إنّ ما يبدو واضحاً هو «أنا جزء من هذه الحفلة الافتراضيّة، مع أصدقائي وزملائي، ونحن نتحدث عن أمور شخصيّة».

لذا، ليس بالمستطاع استخدام إظهار الناس المستمر لبياناتهم الشخصيّة على تلك المواقع، بوصفه دليلاً لموافقتهم على وضعهم تحت المراقبة. ما يوافق الناس عليه هو أن الإنترنت فيها موازاة للعالم الفعلي الذي تختزن رؤوسهم معرفتهم به، ولا

يفهمون على نحو كامل التشعبات والإملاءات كافة من انتقال ذلك العالم الحقيقي إلى الفضاء السبراني[46].

تفضّل شركات كـ «فيسبوك» أن تجري الأمور على ذلك النحو. وتخرج [الشركات] عن طُرُقها المعتادة كي تتأكّد من أنّك لا تفكّر بالخصوصيّة أثناء وجودك على مواقعها، كما تستخدم خدعاً معرفيّة لزيادة ثقتك بها، كأن تعرض عليك صور أصدقائك. تذهب الحكومات أبعد من ذلك بجعلها معظم رقابتها سريّة، فلا يعرف الناس شيئاً عما يحدث. يعطي ذلك تفسيراً للانفصال بين دعاوى الناس بأهمية الخصوصيّة من جهة، واستمرارهم في أفعال تدلّ على العكس؛ ذلك أنّ النُظُم التي نستعملها مصمّمة كي لا تبرز قضية الخصوصيّة[47].

هناك حاجة لإعطاء الناس خيار الخصوصيّة الحق على الإنترنت، والقدرة على فهم ذلك الخيار وتبنّيه. ستضحي الشركات أقل ميلاً لفعل أشياء مريبة ببياناتنا، في حال يجب عليها أن تبرّر نفسها أمام مستخدميها ومستهلكيها[48]. وسيصبح المستعملون أقل إغواءً بدعاوى «المجاني»، إذا عرفوا التكاليف الحقيقيّة[49]. سوف يقتضي ذلك فرض قوانين عن «الحقيقة في المنتج» لتنظيم عمل الشركات، إضافة إلى قوانين مماثلة لتنظيم عمل الحكومة.

في البدايات، سيجب على المواقع الشبكيّة الكشف عما تسعى إليه الأطراف الثلاثة أثناء تتبع زوّار تلك المواقع، ويجب على شركات الهواتف الذكيّة أن تكشف عن المعلومات التي تسجّلها عن مستعمليها. هناك أمكنة كثيرة تُمارَس فيها الرقابة خفية، ويجب جعلها بارزة أيضاً.

مرّة أخرى، ذلك أمر صعب. إذ تشكّل المعرفة والخيار والموافقة طريقة صحيحة للتعامل مع ذلك الوضع[50]، لكننا نعرف لا جدوى تلك الصيغة من سياسات الخصوصيّة المصاغة بلغة قانونيّة مقعّرة؛ وهي التي نوافق عليها عندما نضغط زر «أوافق» على ما يعرض علينا. وعند سابق قصد، جُعِلَت تلك الصيغ طويلة

وتفصيليّة، وبالتالي مملة ومُربِكَة؛ كما أنها لا تنتج موافقة مجدية من قِبَل المستخدم. لا يراودنا شك أيضاً في لا جدوى ظهور تلك النافذة التي تقفز على الشبكة في كل مرّة ندوّن فيها شيئاً ما على «فيسبوك»، لتقول: «ما كتبته سيخزّن في «فيسبوك» ويستخدم للتسويق، كما يعطى إلى الحكومة عندما تطلبه». نحتاج إلى حلّ وسط. ويراودني ظنّ بأنّه يشمل وضع سياسات معياريّة ونوع من الشهادة أو الإجازة لكل طرف ثالث.

إرساء مرجعيات موثوقة للمعلومات

في مناحٍ كثيرة من حيواتنا، نمنح المختصّين نفاذاً إلى معلومات شخصيّة جدّاً عن أنفسنا. وكي نتثبّت من كونهم لا يستعملونها إلا لمصلحتنا، جرى إرساء مفهوم مسؤوليّة المرجعيّة. يتقيّد الأطباء والمحامون والمحاسبون بقوانين تطلب منهم وضع مصلحة زبائنهم فوق مصالحهم الخاصة. تتحكّم تلك القوانين بكيفية استخدامهم المعلومات والسلطة المخوّلة إليهم، ولا تتيح لهم عموماً استعمال المعلومات لأهداف غير ذات صلة. هناك قوانين تفرض على الشرطة متى يستطيع طلب معلومات من المرجعيّات الموثوقة. تخلق علاقة المرجعيّة الموثوقة واجب الاهتمام الذي يتقدّم الالتزامات الأخرى كافة.

نحتاج إلى مرجعيات موثوقة في المعلومات[51]. الفكرة وراء ذلك أنهم سيصبحون شريحة مؤسّساتيّة تمسك بالمعلومات، وتكون عرضة لقيود وحمايات قانونيّة خاصة. يجب على الشركات أن تقرّر إذا ما كانت ستنضوي في تلك الشريحة أم لا. يتشابه ذلك مع المستشارين الاستشاريّين الذين يملكون مسؤوليّة المرجعيّة، فيما لا يملكها السماسرة[52]. وبهدف تحفيز الشركات على التحوّل إلى مرجعيّات موثوقة، تستطيع الحكومات منح إعفاءات ضريبيّة وحمايات قانونيّة للشركات التي تقبل تلك المسؤولية المضافة. ربما نُظِرَ إلى بعض أنواع الأعمال بوصفه مرجعيّة موثوقة بصورة تلقائيّة، ببساطة بسبب الكميات الكبيرة من المعلومات الشخصيّة التي تجمعها بصورة طبيعيّة. يشمل ذلك مقدّمي خدمات الإنترنت، شركات

الخلـوي، مقدمي خدمات البريد الإلكتروني، محـرّكات البحث ومنصّات التواصل الاجتماعي.

مـن شـأن تنظيـم المرجعيّـات إعطاء النـاس الثقـة بـأنّ معلوماتهم لا تسـلّم إلى الحكومة، أو تباع إلى طرف ثالث، أو تسـتخدم ضدّهم. كما يمحض حمايات خاصة للمعلومـات الموكولـة إلى المرجعيّات الموثوقة. ومن شـأنه أيضاً أن يفرض واجبات معينـة في الرعايـة على مـن يدير المعلومـات، كأن يكون مسـتوىً معيّنـاً من الأمن، والتعرّض للتدقيق بصورة منتظمة وما إلى ذلك. يكفل ذلك التنظيم تفعيل الثقة.

وبخطوط مشـابهة، اقترح خبير أمـن الإنترنت دان غير أن يختار مقدّمو خدمات الإنترنـت بين كونهم شركات محتوى أو شركات اتّصالات[53]. فبوصفهم شركات محتوى، يستطيعون استعمال البيانات والاستفادة منها، كما يتحمّلون مسؤولية قانونيّة عنهـا. وبوصفهم شركات اتّصالات، لا يترتب عليهم مسـؤولية حيال المعلومات، لكنهم لا يستطيعون قراءتها.

في العصور الوسـطى، فرضـت الكنيسـة الكاثوليكيّة واجباً صارمـاً من السريّة حيال الذنوب التي يجري الاعتراف بها، معتبرة أن أحداً لن يشارك في طقس الأسرار الإلهيّـة إذا خشي الناس خيانـة الكاهن للأسرار التي يأتمنونه عليها. نحتاج حالياً إلى ثقة من ذلك النوع على الإنترنت.

تحفيز نماذج عمل جديدة

صـارت الرقابـة نموذج العمل عـلى الإنترنت لأنها شـكّلت أسـهل الطرق في الحصـول على المال، مع غياب قوانـين تنظّمها[54]. واسـتمرت نموذجاً للعمل على الإنترنـت بأثـر من انخفـاض التكاليـف، وضخامـة الأربـاح المتوخـاة، و(أقلّه في الولايات المتّحدة) *استمرار* غياب قوانين تنظّمها.

وبوضـع قوانـين تنظّـم جمع البيانـات واسـتعمالها معـاً، ورفع تكلفـة الاحتفاظ بالبيانات، سنحفّز بصورة طبيعيّة نماذج جديدة في العمل لا تكون مستندة إلى الرقابة. وتتوافر القدرات التقنيّة لإنجاز ذلك. هناك بحوث عدّة عن إرسـاء الخصوصيّة في المنتجـات والخدمـات من البدايـة، بمعنى آخر يتعلـق الأمر بتثبيـت الخصوصيّة في تصاميمها[55]. إذ يجب ألا تتتبَّع شركات بطاقات الائتمان تفاصيل مشـترياتنا كافة، كي تصنع فواتيرها وتتجنّب الفساد. يجب على مقدمي خدمات الخلوي ألا يحتفظوا بسـجلات أبديّة عن مواقعنا كي يستمروا في تقديم المكالمات والرسائل النصيّة. من المسـتطاع بناء إنترنت تتضمّن حمايات قويّة لمغفـلي الهويّة. يمكن للنقود الإلكترونيّة أن تكون آمنة وبلا هويّة. تلك الأشياء كلها ممكنة، لكن يجب أن نُطالِب بها.

يجدر الإقرار بأن الآلية المطلوبة ستكون بطيئة. إذ تعتقد الشركات الأكثر توسّعاً في جمـع بياناتنا بـأن فيها إمكانات كامنـة لمداخيل ضخمة تأتي مـن الإعلانات. ربما يصل حجم سـوق إعلانات الإنترنت إلى قرابة 125 بليون دولار عالميّاً، لكنه يمثّل ربـع القيمـة الإجمالية لسـوق الإعلانات. تضـع شركات كـ «فيسـبوك» و«غوغل» نصـب أعينها الأمـوال التي تنفق على إعلانـات التلفزة (40 ٪ من إجمالي السـوق) والصحف والمجـلات (36 ٪)[56]. كذلك وظّفت شركات الإنترنت أموالاً طائلة في «البيانـات الضخمـة» التي تعني جمـع البيانات كافة ثم التفكـير في أوجه التعامل معهـا لاحقاً، ولـن تبدّل توجّهاتها بسـهولة. يطلق الصحافي جايمس كانسـتلر على ذلك «سـيكولوجيّة الاسـتثمار السـابق»[57]، وهو السـبب عينه الـذي يجعلنا نضيّع أمـوالاً بعد أن نكون قد تصرّفنا جيّداً بالأموال التي سـبقتها. مـن الصعوبة الإقرار بأنّك على خطأ، خصوصاً أن تكلفة جمع البيانات وتخزينها منخفضة تماماً.

في اقتصاد السـوق، إذا لم تتمكن شركة ما من وضع نموذج عمل مربح، سيتقدّم الذيـن نجحـوا في ذلك. إذا نجحنـا في رفع تكلفة الرقابة وجمع المعلومات، سـتظهر أنواع من الأعمال لا تسـتند إليهما [الرقابـة وجمع المعلومات]، كما تحل بديلاً للأنواع الموجودة حاضراً وهي تعتمد عليهما.

لنقاوم رقابة الحكومة

حتى الآن، تمثّلت النتيجة الأهم لكشوفات سنودن في أنّها حطّمت الشراكة بين الحكومة والشركات في الرقابة، وهي التي بيّنتها في الفصل 6. قبل سنودن، لم يكن هنالك ضير في تعاون شركة ما مع «وكالة الأمن القومي». إذا طلبت الوكالة إمدادها بنسخ عن كل الحركة الإلكترونيّة على الإنترنت، أو زرعت «أبواباً خلفيّة» في منتج يفترض أنّه يحمي أمن البرامج، كان من المستطاع افتراض أنّ ذلك التعاون سيبقى سرّاً إلى الأبد. وإنصافاً، لم يتعاون الجميع طواعية مع الوكالة. قاوم بعضهم في المحاكم[58]. في المقابل، يبدو أنّ الغالبيّة التي ضمّت صفوفها خصوصاً شركات الاتّصالات الاحتكاريّة التي تهيمن عليها الدولة والشركات العملاقة للإنترنت، رحّبت بإعطاء الوكالة نفاذاً غير مراقب لكل ما طلبته. كان ذلك سهلاً، وفعله الجميع أثناء الحرب الباردة ثم عقب هجمات 9/ 11، بلا ضوضاء.

أخذ ذلك المشهد بالتغيّر. إذ باتت هناك قيمة للانحياز إلى الخصوصيّة ومقارعة «وكالة الأمن القومي»، إضافة إلى حدوث ضرر من التعاون معها. هناك أربعة طرق رئيسة تسلكها الشركات في مقاومة الوكالة، هي: الشفافيّة، والتقنية، والتقاضي، ومجموعات الضغط.

تلجأ مجموعة من شركات الكومبيوتر، كـ«مايكروسوفت» و«ياهوو» و«غوغل» وغيرها، إلى نشر «تقارير شفافيّة» دوريّاً، تعطي فكرة عامة عن عدد طلبات البيانات التي تلقتها الشركات من الحكومة، وكم مرّة استجابت لها[59]. من الواضح أن العلاقات العامة هي المحرّك الأساسي لنشر التقارير، بمعنى القول للجمهور إنّ نسبة صغيرة من بياناته تقدّم للحكومة. ومثلاً، في العام 2013، زعمت شركة «غوغل» أنها سلّمت إلى الحكومة الأميركيّة «بيانات وصفيّة» عن اتّصالات الإنترنت تشمل ما يتراوح بين 1 و2000 مستخدم، إضافة إلى محتويات الاتّصالات لما يتراوح بين 18 ألفاً و20 ألف مستخدم[60]. هناك قوانين تحكم تلك

الأرقام لأنه من غير المسموح للشركات أن تعطي الأرقام الدقيقة، على الرغم من أن بعضها يضغط على الحكومة كي تسمح بإعلان أرقام أكثر دقّة. (تقدّم تقارير «غوغل» أرقاماً أكثر دقّة عن الطلبات من حكومات أخرى، غير الولايات المتّحدة).

وعمدت حتى شركات الاتّصالات والكابل الأميركيّة إلى نشر تقارير شفافيّة، بداية من التقرير الذي أصدرته شركة «كريدو موبايل» (CREDO Mobile) للاتّصالات، في مطلع العام 2014[61]. تملك تلك التقارير قيمة أقل من سواها. مثلاً، أورد تقرير من شركة «فريزون» للاتّصالات أنّها تلقّت قرابة 320 ألف طلب للحصول على البيانات، من قِبَل «قوى إنفاذ القانون» في العام 2013[62]. نعلم أنه كل 3 شهور تتلقّى «فريزون» رسالة واحدة من «وكالة الأمن القومي»، تفرض عليها تسليم «البيانات الوصفيّة» لزبائنها كافة الذين يقدّر عددهم بـ290 مليوناً[63]، فما معنى الـ320 ألفاً؟

تحاول بعض الشركات السير إلى أبعد من ذلك. في 2014، أعلنت شركة «آبل» أنها ستُعلِم كل مستخدم فَرْدٍ بشأن طلب الحكومة بياناته، إلا إذا منعتها الحكومة من ذلك بصورة محدّدة إفرادياً[64]. وشكّلت «مايكروسوفت» و«غوغل» حلفاً قانونيّاً لمقاضاة الحكومة والحصول على مزيد من الشفافيّة[65]. وسارت «ياهوو» في المسار عينه[66].

هناك شركات توظّف أشخاصاً كي يبلغوها سرّاً عن صدور مذكّرات قضائيّة تأمرها بعدم الإفصاح عن تسليم بياناتها إلى جهات رسميّة، ويسمّى هؤلاء «عصافير المذكّرات»[67]. ومنذ 2013، تتضمن تقارير الشفافيّة من شركة «آبل» العبارة التالية: «لم تتلق «آبل» إطلاقاً أمراً تحت الفصل 215 من «قانون باتريوت» في الولايات المتّحدة». وتنقل العبارة فكرة مفادها أنّه لو تلقت «آبل» ذلك الأمر، لما سُمِحَ لها بالإفصاح عن تلقيها إياه، لكن إزالة تلك العبارة تحمل إشارة إلى المتابعين

اليقظين. لم تحسم المحاكم أبداً بشأن قانونيّة تلك الممارسة، وشخصيّاً أُبدي تشككي في نجاعتها، لكنها تمثّل جهداً شجاعاً وذكيّاً[68].

على الجبهة التقنية، ترفع شركات عدّة وتيرة استعمالها للتشفير في اتّصالاتها مع زبائنها ومستخدميها بواسطة الإنترنت، وفي شبكاتها الداخليّة، وفي قواعد بياناتها[69]. بعد أن علم «غوغل» أن «وكالة الأمن القومي» تتنصّت على الجسم الأساسي للروابط الإلكترونيّة في الاتّصالات بين قواعد بياناته؛ عمد إلى تشفير تلك الروابط[70]. وبعد أن علم «ياهوو» أن الوكالة تتنصّت على الصلات الشبكيّة بين مستخدميه ومواقع «ياهوو»[71]، شرع في تشفيرها بالتعاون مع «مايكروسوفت»[72]، التي افترضت أن أمراً مماثلاً يحدث مع مستخدميها ومواقعها[73]. وأخذت شركات كبرى في خدمات البريد الإلكتروني بتشفير ذلك البريد أثناء تنقّله بين قواعد بياناتها[74]. تبذل شركات أخرى جهوداً أكبر في تشفير الاتّصالات التي تربطها بزبائنها ومستخدميها[75]. اعتمدت هواتف الـ «آي فون» والـ «آندرويد» التشفير كإجراء أساسي[76]. بات «غوغل» يقدّم خيار التشفير بين طرفي التراسل بواسطة بريد «جي ميل»، على الرغم من حدسي بأن ذلك الخيار لن يروج كثيراً؛ لأن المستخدمين لن يتمكّنوا من البحث في رسائلهم وتصنيفها، إذا بقيت مشفّرة[77].

في المحاكم، يجب على الشركات أن تترافع لمصلحة جمهور مستخدميها. يجب أن تطلب مذكّرات من المحاكم لكل عملية وصول إلى بياناتها، وأن تقاوم قضائيّاً في حال تلقّيها مذكّرات تتوسّع في النفاذ إلى بياناتها بشكل مفرط. يحدث بعضٌ من ذلك منذ مدّة. في العام 2008، حارب «ياهوو» سراً «وكالة الأمن القومي» في المحاكم، وعاند لفترة طويلة قبل أن ينضم إلى برنامج «بريزم»(*) في الوكالة[78]. في 2012، أخفق «تويتر» في معركته ضد طلب حكومي بتسليمها معلومات تتصل بنشطاء

(*) راجع الفصل 6.

في حركة «احتلوا وول ستريت»[79]. في 2014، خاض «فيسبوك» معركة قضائيّة ضد مدعي عام مقاطعة نيويورك الذي طلب تسليم رسائل خاصة وصور ومواد مُشابِهة؛ لاستعمالها في بحث جنائي عن فساد في مؤسّسة «الضمان الاجتماعي»[80].

بوسع الشركات أن تفعل أكثر من ذلك لدعم جهود التقاضي. إذ يجب أن تحتفظ بملخّصات قضائيّة عن آراء الخبراء الذين تستشيرهم المحاكم قانونيّاً بشأن قضايا ربما شكّلت سوابق قضائيّة تمسّ تلك الشركات. في 2013، طلب الـ «إف بي آي» المفتاح الشامل للملفات مستخدمي البريد الإلكتروني كافة لشركة «لافابيت»، بهدف الوصول إلى بريد أحد المستخدمين. لم ترفع أيٌّ من الشركات الكبرى للبريد الإلكتروني، كـ «غوغل» و«مايكروسوفت» و«ياهوو» وغيرها، دعاوى قضائيّة بشأن ذلك التصرّف[81]. لِمَ لَمْ تفعل؟ يجب على الشركات أن تدرك أن ذلك الشأن يطالنا جميعاً.

مرّة أخرى، يشكّل الطابع الدولي للإنترنت ثنية معقّدة في ذلك المجال. من المستطاع أن تختار شركة ما الانصياع إلى الطلبات القانونيّة للبيانات في بلدها، فماذا عن بقية البلدان؟ في أربع مناسبات في السنوات القليلة التي تلت العام 2000، انصاع محرّك البحث «ياهوو» لطلب من الحكومة الصينيّة بيانات عن أفراد من مستخدميه، استُخدِمَت في توقيفهم وسجنهم بتهمة «التخريب» و«كشف أسرار الدولة»[82]. هل يجب على «ياهوو» الانصياع؟ هل من فارق إذا كان نظام قمعي ما (...) على علاقة طيّبة مع الولايات المتّحدة؟ تزعم مجموعة من شركات الإنترنت أنّها لا تكون تحت سلطة البلدان التي لا مكاتب لها فيها. ربما لا تستطيع شركة أميركيّة أن تقاوم القانون الصيني، لكنها تستطيع مقاومة بلدان أخرى أصغر وأقل قوّة. بطرق كثيرة، تستطيع تلك الشركات أن تختار أي البلدان تطيع القانون فيها، وأيّها لا تفعل ذلك. يجب عليها أن تختار تعظيم خصوصيّة مستخدميها إلى أقصى حدّ.

في الأروقـة السياسـيّة، يجـب على الـشركات أن تسـتعمل نفوذها السـياسي. إذ تنخـرط شركات كـ «مايكروسـوفت» و«فيسـبوك» و«غوغـل» وغيرهـا، بنشـاط مـع مجموعـات الضغط السـياسي، بهدف فرض قيـود قانونيّة على ممارسـة الحكومة الأميركيّـة للرقابـة[83]. إنّـه أمـر جيّـد، لكن هنـاك حاجـة إلى مزيد منـه. في أغلب الأحيـان، تـأتي الحجج السياسـيّة الأكثـر إقناعاً مـن شركات مهتمّـة بالوصول إلى خلاصات الأمور.

كذلـك يجب عدم الإفـراط في ذلك كلـه. إذ إن مصالح الـشركات ربما تقاطعت مرحليّـاً مـع مصالـح الخصوصيّة لـدى المسـتخدمين، لكنهما ليسـا متحالفـين دائماً. لسنوات طويلة، قاتلت الشركات ضد القوانين التي تحدّ من قدرتها على جمع البيانات واسـتخدامها. بـذل الاتحاد الأوروبي جهـوداً من أجل إقرار تشريعـات أكثر صرامة وحداثة في ذلك الشأن، لكنه جوبه بحملات ضارية من مجموعات الضغط التي تعمل لمصلحة شركات الإنترنت الأميركيّة غير الراغبة في التوقّف عن جمع المعلومات[84]. إنّ هـذه الهيكليّـة الصاعدة حـاضراً في الوقوف بوجـه «وكالة الأمـن القومي»، هي أقرب لكونها حملة لتغيير رؤية المستخدم، من كونها جهوداً تهدف لإيجاد حلّ لمشكلة الخصوصيّة. لذا، نحتاج أيضاً إلى قوانين قويّة تضبط الشركات أيضاً.

نحو وثيقة «ماغنا كارتا» جديدة

دعا المهندس الإلكتروني السـير تيـم بيرنرز لي، وهو مبتكر «الشـبكة العنكبوتيّة الدوليّـة»، إلى صوغ وثيقة «ماغنا كارتا» (Magna Carta)(*) جديدة تعمل على تقييد الحكومـات والشركات معاً[85]، وتفرض مسـؤوليّات على الشركات التي تعمل في عـصر المعلوماتيّة، فـلا تكتفي بالحقوق وحدهـا[86]. وعمليّاً، ليسـت تلك المقارنة

(*) في العام 1215، أرغم بارونات إنكلترا الملك جون الأول على توقيع وثيقة الـ"ماغنا كارتا" (ترجمتها حرفيّاً: "الشرعة العظيمة") التي تضمن الحريّات الأساسيّة في المجتمع. وتعدُّ الوثيقة صيغة تأسيسيّة أولى للديمقراطيّة في الغرب.

التاريخيّة عظيمة، لكن تلك الفكرة العامة جديرة بأن تكتشف. وتمثّل أيضاً الفكرة الأساسيّة التي أدعو لها في هذا الكتاب.

هل تذكر أنّني في الفصل 4، وصفتُ العلاقة بين الشركات والمستخدم بأنها إقطاعيّة؟ يرجع ذلك لكونها علاقة مُغرِضَة وأحاديّة الجانب. إذ تتأسّس على اتفاقيّة للمستخدم النهائي جرت صياغتها بصيغة قانونيّة مربكة للعقل، كما تستطيع الشركة تغييرها وفق رغباتها. تاريخيّاً، كانت الإقطاعيّة شبيهة بذلك، بمعنى أن اللوردات امتلكوا الحقوق كافة، فيما لم يفرض عليهم سوى النزر اليسير من المسؤوليّات. في أوروبا القرون الوسطى، أدّى صعود الدولة المركزيّة وحكم القانون، إلى إعطاء الإقطاع المرونة التي كان يفتقدها. وفي 1215، صارت الـ «ماغنا كارتا» أول وثيقة حديثة تصون وتحتضن فكرة أن شرعيّة الحاكم تأتي من أتباعه، وأخضعت الملك لحكم القانون. في البداية، ألزمت الوثيقة الملوك بمسؤوليّات حيال اللوردات التابعين لهم، ثم توسّعت تدريجيّاً لتضع المجتمع على طريق حكم الشعب بالشعب وللشعب.

في القرن الثامن عشر، عندما شرعت الدول في إدراك أن سلطتهم في الحكم تنبع من الشعب كلّه، سادت الفلسفة السياسيّة للمفكر الإنكليزي توماس هوبز، الذي دافع عن فكرة تضحية الشعب بالسلطة والحريّة ليضعها بيد متسيّد مطبوع على الخير يكون واجباً عليه إعطاء الشعب خدمات متنوّعة، بما فيها الأمن[87]. وحاجج الفيلسوف الإنكليزي جون لوك ضد تلك الفكرة واصفاً تلك الصيغة من العلاقة بين المتسيّد والشعب بأنها غير عادلة وغير متوازنة، معتبراً أنّ الحكومات تستمد سلطاتها من «موافقة المحكومين»[88]. أشعلت مفاهيم لوك الثورات في إنكلترا وفرنسا وأميركا، وأدّت إلى صوغ «إعلان حقوق الإنسان والمواطن» في فرنسا، و«وثيقة الحقوق» في الولايات المتّحدة.

"إعلان مدريد للخصوصيّة" (2009)[89]

يغتنم المجتمع المدني فرصة اللقاء السنوي 31 لـ"المؤتمر الدولي لمفوّضي الخصوصيّة وحماية البيانات" كي:

1 - يجدّد الدعم لإيجاد إطار عن «الممارسات العادلة في المعلومات» يفرض واجبات على أولئك الذين يجمعون المعلومات الشخصيّة ويتعاملون معها، ويعطي حقوقاً لمن جُمِعَت معلوماتهم الشخصيّة.

2 - يجدّد الدعم لإيجاد سلطات مستقلّة لحماية البيانات، تتخذ قراراتها ضمن إطار شرعي، بشفافيّة ومن دون مصلحة تجاريّة أو تأثير سياسي.

3 - يجدّد الدعم لإيجاد تقنيّات لتمكين الخصوصيّة، يكون من شأنها تقليص أو إنهاء عمليات جمع معلومات معرّفة بأنّها شخصيّة، وكذلك وضع تقييمات لتأثير الخصوصيّة بطريقة مجدية تفرض الانصياع لمعايير الخصوصيّة.

4 - يحضّ البلدان التي لم تقر «ميثاق مجلس أوروبا 108» مع «بروتوكول 2001» أن تفعل ذلك بأسرع وقت ممكن.

5 - يحضّ البلدان التي لم ترسِ إطاراً شاملاً لحماية الخصوصيّة وسلطة مستقلّة لحماية البيانات أن تفعل ذلك بأسرع وقت ممكن.

6 - يحضّ البلدان التي أرست أطراً قانونيّة لحماية الخصوصيّة أن تضمن التنفيذ الفعّال وتدعمه، وأن تتعاون على المستويين الدولي والإقليمي.

7 - يحضّ البلدان على التثبّت من إشعار الأفراد بسرعة عندما تتعرض معلوماتهم الشخصيّة للانكشاف غير المناسب، أو للاستعمال بطريقة لا تتلاءم مع تجميعها.

8 - يوصي ببحوث شاملة عن مدى مواءمة تقنيات إخفاء هويّة البيانات، للتثبت من كونها عمليّاً تمثّل طرقاً تحمي الخصوصيّة وإغفال الهويّة.

9 - يدعو إلى وقف تطوير أو تنفيذ نُظُم جديدة في الرقابة العامة، بما فيها التعرّف إلى الوجه، والتصوير المسحي للجسم كاملاً، المعرِّفات البيولوجيّة، واللواحق المغنطة بطريقة «ريفد»؛ مع وضعها قيد تقييم شامل وشفاف من قِبَل سلطات مستقلّة، وبنقاش ديمقراطي.

10 - يدعو إلى تأسيس إطار دولي جديد لحماية الخصوصيّة، مع المشاركة الكاملة للمجتمع المدني، يكون مستنداً إلى حكم القانون، واحترام الحقوق الأساسيّة للإنسان، ودعم المؤسّسات الديمقراطيّة.

في كتابها بعنوان موافقة المتّصلين بالشبكات، أثارت الصحافيّة والمدافعة عن الحقوق الرقميّة ريبيكا ماكينون، النقطة التالية: «لن تكون أي شركة مثاليّة، ولن يوجد متسيّد مثالي، مهما حسُنَت النوايا والفضائل عند الملك أو الملكة أو الديكتاتور المطبوع على الخير. وتلك هي النقطة تماماً، بمعنى أن عقدنا الاجتماعي مع العواهل الرقميّين تجري على مستوى بدائي، وهوبزي [نسبة للمفكر هوبز] وملكيّ. إذا كنّا محظوظين، يكون العاهل جيّداً ونصلّي كي لا يكون ابنه أو خليفته المختار شيطاناً. هناك سبب لكون معظم الناس لم يعد يقبل بذلك النوع من التسيُّد. حان الوقت كي نرتقي بالعقد الاجتماعي المتعلّق بالحوكمة الرقميّة لحيواتنا إلى المستوى الذي دعا المفكّر لوك إليه. ويعني ذلك أنّ إدارة هويّاتنا ودرجة وصولنا إلى المعلومات، يمكنها أن تعبّر بأصالة وإخلاص عن موافقة المتّصلين بالشبكات»[90].

تتمثّل الفكرة في أنّ صوغ «ماغنا كارتا» جديدة تكون أشد تركيزاً على المؤسّسات التي أساءت استعمال السلطة في القرن 21، سيكون لها تأثير يشابه نظيرتها التاريخيّة. هناك بعض الوثائق اقتربت من تلك الفكرة. إذ ما زال «إعلان مدريد للخصوصيّة» (2009) يعدُّ الصيغة الأشد تماسكاً لحقوق الخصوصيّة في العصر الحديث.

15

حلول للبقيّة منا

تمثّل الرقابة مشكلة قانونيّة وتقنيّة. وغالباً، تصل الحلول التقنيّة إلى يد المستخدم. نستطيع استعمال تقنيّات للخصوصيّة وإغفال الهويّة لحماية بياناتنا وهويّاتنا. تتسم تلك التقنيّات بالفعاليّة، لكن يمكن خنقها بواسطة أوامر حكوميّة سريّة. ويجب أن نخوض معركة سياسيّة في ذلك أيضاً.

تتطلّب الحلول السياسيّة جهداً جماعيّاً، لكنها غالباً تجري ضمن بلدان محدّدة. وتميل الحلول التقنيّة إلى العالميّة. إذا صمّمت «مايكروسوفت» نظام تشغيلها «ويندوز» وزوّدته بتشفير شامل، وإذا قرّر «فريق العمل على هندسة الإنترنت»(*) (Internet Engineering Task Force) أن كل ما يمر في الإنترنت يجب أن يشفّر، تطال تلك المتغيّرات كل شخص في العالم عند استخدامه تلك المنتجات والبروتوكولات.

إذاً، المسألة هي أن السياسة بإمكانها تخريب التقنية، كما تستطيع التقنية أن تخرّب السياسة. لا يتقدّم أحدهما على الآخر. إذا سعينا للإصلاح، يجب علينا القتال على جبهتي السياسة والتقنية معاً. ولا يتّصل ذلك بالحكومات والشركات. هناك الكثير مما نستطيع نحن الشعب أن نفعله.

(*) هي هيئة دوليّة من مهندسي الإنترنت وتقنيّيها ومشغّليها وبحّاثتها تعنى بتطوّر هندسة تلك الشبكة. وتأسّست في 1986، وهي مفتوحة أمام الجمهور.

مقاومة الرقابة

كتب أستاذ القانون البروفسور آيبن موغلن: «إذا لم نرتكب أخطاءً، يكون لدينا الحق في فعل كل ما بوسعنا للحفاظ على التوازن التقليدي بيننا وبين السلطة المتنصّتة. نملك الحق في أن نكون غامضين. نملك الحق في الغمغمة. نملك الحق في التحدّث بلغات لا تفهمها الحكومة. ونملك الحق في أن نلتقي في الزمان والمكان الذي يناسبنا»[1]. إذا جلس رجل بوليس ضمن مدى السمع ليتنصّت علينا، يكون من حقنا الانتقال إلى مكان آخر. إذا تمترس قرب بيتك ضبّاط الـ «إف بي آي» في شاحنة تعجّ بالكاميرات، فمن حقّك تماماً أن تسدل الستائر والحُجُب.

وعلى غرار ذلك، هناك طُرُق متنوّعة تمكّننا من حماية بياناتنا بأنفسنا، وأن ندافع عن أنفسنا ضد الرقابة. وسأصنف تلك الطُرُق ضمن مجموعات مستقلّة[2].

تجنّب الرقابة. تستطيع أن تغيّر عاداتك كي تتجنّب الرقابة. تستطيع أن تدفع نقداً لشراء بعض الأشياء بدلاً من استعمال بطاقة الائتمان، أو أن تتعمّد تغيير طريقك لتجنّب كاميرات مراقبة المرور. تستطيع التوقّف عن إنشاء صفحات على «فيسبوك» لأطفالك، وتمتنع عن وضع تعريفات على صورهم المنشورة على الشبكة. تستطيع التوقف عن استخدام «مفكّرة غوغل» وأنوع البريد الإلكتروني المستند إلى الـ «ويب»، إضافة إلى تجنّب تخزين المعلومات في «السحب الرقميّة». تستطيع استعمال محرّك البحث «داك داك غو» في التفتيش عن المعلومات على الإنترنت. تستطيع ترك هاتفك الخلوي في المنزل، وهي طريقة سهلة لتجنّب التتبع. بتحديد أكثر، تستطيع ترك هاتفك الخلوي وحاسوبك عندما تسافر إلى بلدان كالصين وروسيا، وتكتفي باستخدام معدّات مستأجرة.

تستطيع تجنّب التشغيل الأوتوماتيكي لنُظُم الرقابة بتعمّدك عدم تشغيل خوارزميات التتبّع لتلك النُظُم. مثلاً، تستطيع إبقاء تعاملاتك الماليّة النقديّة تحت الحدّ الذي يُطلَب فيه من المؤسّسات الماليّة تبليغ الحكومة عنه. بإمكانك أن تنأى

بنفسـك عن نقـاش مواضيع معيّنة عبر البريد الإلكتروني. في الصين، تسـود الرقابة الأوتوماتيكيّة ما يضطر الناس أحياناً إلى كتابة رسـائل على الورق، ثم إرسـال صور عن تلك الرسـائل بواسـطة البريـد الإلكـتروني. لا ينفع ذلك الإجـراء في مواجهة الرقابـة الموجّهـة، لكنـه يصعّـب الأمور عـلى الرقابـة الأوتوماتيكيّة. وتعمـل تقنية الـ «ستِغانوغرافيا» (Steganography)، ومعناها كتابة معلومات سراً ضمن رسائل أو صور عاديّة-، ضمن أفق مشابه.

صـدّ الرقابة. يشـكّل ذلك الطريـق الأكثر أهمية لحماية أنفسـنا. ربما تملك «وكالة الأمن القومي» ميزانية تفوق مجموع ما يرصد لوكالات التجسـس كافة لدول العالم بأسره، لكن ذلك لا يجعلها سـحراً، وكذلك الحال بالنسـبة لبقية وكالات التجسّس في البلـدان كلهـا. يعتمد التجسّـس الفعّال عـلى الاقتصاد والفيزيـاء والرياضيّات. وتسـتطيع الوكالات الأمنيّة في العالم كله هزيمتك إذا ركّزت عليك بشـخصك، إلا أن الرقابـة العامة تعتمد على الوصول السـهل لبياناتنـا ومعلوماتنا. ويتمكن الدفاع الجيّـد إرغام من يسـعون إلى رقابتنا عـلى انتقاء أهدافهم؛ لأنهم ببسـاطة لا يملكون موارد كافية لاستهداف كل شخص على حدة.

هنالـك مـا يسـمّى «تقنيّـات تعزيـز الخصوصيّـة» (Privacy Enhancing Technologies) [3] ويشـار إليهـا بالاسـم المختـصر «بـت» (PET)، تسـتطيع أن تسـاعدك في صدّ الرقابة العامة. هناك تقنيّات كثيرة تسـاعدك في حماية بياناتك. ثمة مُكوّنـات رقميّة أساسـيّة للاتّصـال بالإنترنت، يمكن إدخالهـا في محـرّكات البحث بهـدف تقـصّي المواقـع التي تتعقّبـك أثنـاء تجـوالك على الإنترنت وصدّها، وهي تشـمل «لايـت بيـم» (Lightbeam) و«برايفـسي بادرجـر» (Privacy Badger) [4] و«دسكونكت» (Disconnect) و«غوسـتري» (Ghostry) و«فلاش بلوك» (Flash Block) وغيرهـا[5]. تذكّر أن خيـارات خصوصيّة التجوّل الموجـودة في متصفحّك تتولّى حذف البيانـات موضعيّاً[6]. ويعني ذلك أنها تفيد في إخفاء زياراتك للمواقع الإباحيّة عن أعين زوجتك، لكنها لا تصدّ عمليات ملاحقتك على الإنترنت.

التقنيّـة الأكثـر أهمية بين أنـواع الـ «بِت» هي التشـفير. ويعطيـك برنامج «بيت لوكر» (Bit Locker) الذي تصنعه «مايكروسوفت»[7]، ونظيره «فايل فولت» (File Vault) مـن «آبـل»[8]، القدرة على تشـفير القرص الصلب بسـهولة فائقة وشـفافيّة كاملـة. (في العام 2014، كنت أنصـح ببرنامج «تروكريبـت» (TrueCrypt)، لكن المُطوّرين توقفوا عن تطويره في تلك السنة تحت ظروف غامضة، ومن الصعب على الجميع إعطاء رأي حاسـم بشـأنه)[9]. تستطيع اسـتخدام برامج تشفير «الدردشة» بواسطة الإنترنت كـ «أوف زي ريكورد» (Off the Record)، وهو سهل الاستعمال وآمـن تماماً[10]. يسـتأهل برنامج «كريبتـوكات» (CryptoCat) بعـض التفكير. إذا كنـت تخـزّن معلوماتك على «سـحابة» رقميّة، اخـتر شركة تعطيك خيار التشـفير. وشـخصيّاً، أنـا معجـب ببرنامـج «سـبايدر رووك» (SpiderRoak)، لكـن هنـاك برامـج أخـرى. هناك برامج لتشـفير الصوت على الإنترنت كـ«سـايلنت سـيركل» (SilentCircle) و«تورفون» (TORFone) و«ريد فون» (RedPhone) و«بلاك فون» (Blackphone).

حـاول إدخال مُكـوّن رقمي للاتّصـال بالإنترنت في البريـد الإلكتروني، كـ «بي جي بي» (PGP). وحاضراً، يقدّم «غوغل» بريداً إلكترونيّاً مشفّراً لمستخدميه، وعلى الرغم من أنه يربك تنظيم الرسائل وعمليات أخرى، فإنّه يزيد الخصوصيّة بما يجعله مجدياً[11].

يوصـف «تي إس إل» (TSL)- واسـمه السـابق «إس إس إل» (SSL)- بأنّـه بروتوكول يساعد على تشفير بعض عمليات التنقّل على الإنترنت[12]. إنّه ما يحدث أوتوماتيكيـا في خلفيّـة المشـهد، عندمـا تـرى رمـز «إتـش تي تي بي إس» (https) في بدايـة العنوان الإلكتروني للموقع الشـبكي، بدلاً مـن «إتش تي تي بي» (http). يقدم العديد من المواقع الإلكترونية ذلك كخيار، ولكن ليس كصيغة افتراضية صحيحة. تأكـد أنه يعمل بصورة مسـتمرة حين يمكنك ذلك، بوضع مكـوّن رقمي للاتّصال

في محرّك البحث بالإنترنت، يسمّى «إتش تي تي بي إس إيفري وير» (HTTPS Everywhere)[13].

ما سبق ليس لائحة حصريّة؛ لأن وضعها يستلزم وضع كتاب سرعان ما تصبح معلوماته قديمة خلال شهور قليلة. إذ تتبدّل التكنولوجيا باستمرار، وعليك أن تذهب إلى الإنترنت للبحث عما يوصي به الخبراء[14].

لن أتولّى قيادتك. هنالك عدد كبير من تقنيّات الـ «بِت» تتخطى القدرات التقنية للقارئ العادي لهذا الكتاب. على وجه الخصوص، من المربك تماماً استعمال المكوّن الرقمي «بي جي بي»[15]. إن تقنيّات التشفير الأشد فعاليّة هي تلك التي تعمل في الخلفية حتى عندما لا تحس بوجودها، كـ «إتش تي تي بي إس إيفري وير» وتقنيات تشفير القرص الصلب. في الفصل 14، ناقشت أشياءً تفعلها الشركات لتأمين بيانات مستخدميها. هناك أشياء أكثر من ذلك بكثير تجري في الكواليس. ثار سخط المؤسّسات المعياريّة الكبرى التي تدير الإنترنت بسبب رقابة الحكومة، إلى حدّ أنها تسعى إلى جعل التشفير موجوداً في الأمكنة كافة على الإنترنت[16]. ويؤمل أن تكون خيارات أخرى باتت متاحة عندما ينشر هذا الكتاب.

يستعصي معظم «البيانات الوصفيّة» على التشفير. لذا، تستطيع تشفير محتويات بريدك الإلكتروني، لكن يجب فك التشفير عند جهتي الإرسال والتلقي كي يعمل البريد الإلكتروني. وعلى نحو مُشابه، من المستطاع تشفير مكالماتك الصوتيّة، لكن إنجاز الاتّصال يوجب عدم تشفير الرقم الذي تطلبه، وموقع هاتفك، وأرقام هويّة هاتفك. وتستطيع تشفير معلومات بطاقتك الائتمانيّة عندما ترسلها بواسطة الإنترنت إلى أحد المحلاّت، تحتاج الشركة إلى اسمك وعنوان منزلك كي ترسل مشترياتك إليك.

وأخيراً، لا يحمي التشفير حاسوبك أثناء استعماله؛ فيبقى عرضة للاختراق من قِبَل المجرمين أو الحكومة. لكن، مرّة أخرى، يكون الشرط لحدوث ذلك أن تكون

مستهدفاً، لا أن تُصاب ضمن ضربة عامة. وتعني تلك الأشياء كلّها أنّ التشفير جزء مهم من الحل، لكنه ليس الحل بأكمله.

حاضراً، يشكّل برنامج «تور» (TOR) أفضل أداة لحماية سريّة هويّتك على الإنترنت. يتميّز بالسهولة في الاستعمال، وبقدر ما نعرف فإنّه آمن. وكذلك من المستطاع استعمال هويّات بديلة للتهرب من الرقابة والحجب. يستطيع برنامج «أونيون شير» (Onionshare) إرسال الملفات بواسطة الإنترنت مع إغفال الهويّة، بفضل برنامج «تور»[17]. وعلى رغم آراء مُعارِضة، تمثّل الهويّات البديلة للخوادم وسيلة ناجعة لإغفال الهويّة[18].

ثمة أشياء بسيطة تستطيع استخدامها في صدّ الرقابة. تستطيع إيقاف خيار «خدمات الموقع» على هاتفك الذكي عندما لا تكون بحاجة إليها. حاول الحصول على معلومات كافية قبل اتّخاذ قرار أن تضع على هاتفك تطبيقاً رقمياً يطلب موقعك وبيانات أخرى. بإمكانك التوقّف عن وضع معلومات مُعرّفَة في حساباتك على المواقع العامة. عندما التقى إدوارد سنودن الصحافيّين للمرّة الأولى في هونغ كونغ، أرغمهم على وضع هواتفهم النقّالة كلها في ثلاجة لحجب إشاراتها الصادرة والواردة، فلا تكون الهواتف أدوات إصغاء تعمل عن بُعدْ[19].

أحياناً، يكون صدّ الرقابة أمراً سهلاً تماماً. يكفي وضع لاصق فوق كاميرا الكومبيوتر فتكف عن التقاط الصور لمصلحة طرف استطاع أن يسيطر عليها عن بُعد. بإمكانك عدم وضع عنوان المُرسِل على مغلّف الرسالة البريديّة الورقيّة، فتقلّص من المعلومات التي يعرفها مكتب البريد عنك. تستطيع استئجار شخص ليسير خلف سيارتك فلا تلتقط كاميرات المراقبة لوحة أرقامها الخلفيّة، وهو ما يفعله البعض في طهران[20]. أحياناً، يكون الأمر بمثل سهولة أن تقول «لا»، المقصود بذلك هو النأي بالنفس عن إعطاء معلومات شخصيّة على الاستمارات، وعدم إعطاء رقم هاتفك الخلوي لعامل المبيعات في المخزن وغيرها.

بعض أنواع صدّ الرقابة تكون غير مشروعة: ليس مسموحاً لك بأن تغطّي فعليّاً لوحة أرقام سيارتك؛ كما أن بعضها مستهجن اجتماعيّاً كالتجوّل بين الناس مع ارتداء قناع؛ فيما أنواع أخرى ربما تجعلك عرضة للاستهزاء، كطلي الوجه بالصبغة كي لا تتعرّف الكاميرات إليه[21]، أو ارتداء ملابس معيّنة لتضليل طائرات الـ «درون»[22].

تشويه الرقابة. أنا أستخدم محرّك بحث عملت على ضبط إعداداته كي تمسح الـ «كوكيز» في كل مرّة أُغلِقه فيها، وهو ما يتكرّر مرّات عدّة يوميّاً. ولا يعني ذلك سوى أنني لا زلت خاضعاً للرقابة، لكن صار من الصعب تنسيق كل تلك الرقابات الصغيرة التي تجريها الـ «كوكيز» معاً لتعمل ضدّي، وكذلك لا تتبعني الإعلانات. عندما أتسوّق من مخازن «سافواي»، أستخدم بطاقة صديقتي، وهي بطاقة من النوع التي يصدرها المخزن نفسه لمن يكرّر الشراء منه. ويؤدّي ذلك إلى تشويه معلومات الرقابة عنها.

أحياناً يسمّى ذلك «تعمية»، وتشمل خدعاً كثيرة تستطيع أنت ابتكارها، عندما تبدأ بالتفكير في الأمر[23]. يمكنك أن تتبادل بطاقات «المقرّبون» التي تعطيها المخازن الكبرى إلى زبائنها الدائمين مع أصدقائك وجيرانك. تستطيع أن ترتدي ملابس تجعل مظهرك ملتبساً. في رواية **الأخ الصغير** (Little Brother) للكاتب كوري دوكتورو، يعمد بطل الرواية إلى وضع حجارة في حذائه كي يغيّر مشيته ويخدع نُظُم التعرّف إلى طريقة المشي[24].

هناك أمان في الأرقام أيضاً. كلما كان هنالك أمكنة في العالم تعمل فيها تقنيّات الـ «بِت» على إنقاذ الناس، وزاد استخدامنا لها؛ صارت أكثر أمناً. يشبه ذلك مغلّفات الرسائل الورق. لو تكاثر عدد مستخدمي البطاقات البريديّة إلى حدّ أن تصير هي القاعدة الأساسيّة في التراسل، يصبح مستخدمو المغلّفات موضع شبهة. لكن، لأن معظم الناس يستعمل المغلّفات الورق، لا يصار إلى الاشتباه في من

يستعملون مغلّفات الورق للحصول على الأمان لرسائلهم. ينطبق ذلك خصوصاً على برامج إخفاء الهويّة كـ «تور»، الذي يعتمد على عدد الناس الذين يستخدمونه كي يستطيع إخفاء هويّتهم جميعاً.

تستطيع أيضاً، وأنا أعرف أشخاصاً يفعلون ذلك، البحث عن أسماء عشوائيّة على «فيسبوك» كي تضلّل من يسعى إلى معرفة مَنْ تعرفهم فعليّاً. في أفضل الحالات، يمثّل ذلك حلاً جزئيّاً؛ لأن تحليل المعلومات يحتاج إلى التمييز بين الإشارات التي تحمل بيانات، والإشارات ذات الدلالة العشوائيّة التي تشبه الضوضاء؛ ما يعني إضافة مزيد من الضوضاء وتصعيب مهمة تحليل البيانات.

تستطيع أن تعطي معلومات مغلوطة عنك للاستمارات على الـ «ويب»، أو كلما طُلِب منك. (تذكّر أنّ أطفالك يفعلون ذلك طوال الوقت)[25]. لمدّة سنوات، قبل زمن من رواج عمليات تتبّع المستهلكين، كانت سلسلة مخازن «راديو شاك» (Radio Shack) تطلب روتينيّاً من الزبائن أرقام هواتفهم وعناوين بيوتهم. رفضت ذلك فترة، لكن ذلك بدا مستهجناً اجتماعيّاً[26]. وبدلاً من ذلك، اعتدت أن أعطي العنوان التالي: «9800، سافاج روود، كولومبيا، ولاية ميريلاند، 20755»، وهو عنوان مقر «وكالة الأمن القومي». وعندما أخبرت زميلاً لي بالأمر، أعلمني أنّه يعطي العنوان الوهمي التالي: «1600، بنسلفانيا آفنيو، واشنطن، دي سي»، مصرّاً على أن أحداً لم يكشفه.

في وسعك الحصول على بطاقة ائتمان باسم ثانٍ. لا شيء سريٌّ في الأمر، إذ يكفي أن تطلب من شركة بطاقات الائتمان بطاقة أخرى باسم مغاير، مع بقائه مربوطاً بحسابك. وإذا لم يطلب البائع بطاقة الهويّة منك، تستطيع استعمال تلك البطاقة.

يعطي الخداع نتائج مذهلة إذا مورس بتقشف وتقطّع. أتذكّر قصة عن مجموعة نشطاء مغاربة. كانت الشرطة السرية تتعقّب كل من لا يملك هاتفاً خلوياً منهم، ما يعرضه للضرب أيضاً. وعمد أعضاء المجموعة إلى اقتناء خلويات، لكنهم كانوا

يتركونهـا في المنازل عندمـا يريدون إخفاء تحرّكاتهم فعليّاً. وبصـورة أكثر تعمياً، إذا سدّت على الرقابة المعادية الأقنية كافة، تنسد أمامك إمكانيّة خداعها أيضاً.

كسر الرقابة. استناداً إلى التكنولوجيا، تستطيع كسر أنواع من نُظُم الرقابة. بإمكانك قطع خطوط الكهرباء عن أجهزة مراقبة السرعة في الشوارع. تستطيع رشّ طلاء على عدسات كاميرات المراقبة. إذا كنت «هاكر» متمرّس، تستطيع تعطيل نُظُم الرقابة على الإنترنت، حذف أو تشويش قواعد بيانات الرقابة، أو ممارسة أنواع أخرى من التخريب. لكن، توخّ الحذر لأن معظم الأشياء التي وردت توآ هي غير قانونيّة.

بعض تلك السُبُل أكثر صعوبة من بعضها الآخر. سوف ينجز بعضنا أشياء أكثر من بعضنا الآخر. هناك من يعمد إلى إدخال معلومات عشوائيّة في استمارات الإنترنت. حفنة ضئيلة من الناس- أنا لا أعرف سوى شخص واحد- تُجري عمليات بحث عشوائيّة على «غوغل» للتشويش على بروفايلاتها في قواعد بيانات ذلك المحرّك. يترتّب على كثير من تلك الأشياء أكلافاً اجتماعيّة أو ماليّة أو هدراً للوقت، إضافة إلى العبء النفسي للوقوع في براثن البارانويا على مدار الساعة. شخصيّاً، نادراً ما أتقدّم للحصول على بطاقات «المقرّبون» التي تعطيها المخازن الكبرى إلى زبائنها الدائمين، ما يعني حرماني من التخفيضات التي تمنح إلى تلك البطاقات. ولا أستخدم بريد الـ «جي ميل»، كما لا أدخل إلى بريدي الإلكتروني من الـ «ويب». لا أملك حساباً شخصيّاً على «فيسبوك»، ما يعني أنني غير متّصل بأصدقائي بالطُرُق التي يتيحها ذلك الموقع. لكنني أحمل هاتفي الخلوي معي معظم الوقت، ويعني ذلك أن شركات عدّة تتبعني. ويستطيع كل امرئ اختيار ما يحلو له من السُبُل.

يجب على كل منا بذل قصارى جهده، استناداً إلى الإيمان بأن الخصوصيّة أمر مهم وأنّه يجب أن نمارس حقوقنا تحت طائلة فقدانها[27]. لكن، بحق السماء، لا

تعبّئوا تلك الاستمارات السخيفة على الإنترنت، إذا كنتم لا تعرفون إلى أين ستصل بياناتكم.

مساعدة رقابة الحكومة

ربما بدا أن إطلاق نداء لمساعدة جهود الحكومة في الرقابة أمر لا مكان له في الكتاب، لكن أصيخوا السمع إليّ قليلاً.

هنالك حاجات مشروعة للرقابة الحكوميّة، تنبع من حاجات الاستخبارات وقوى إنفاذ القانون معاً، ويجب أن نقرّ بذلك. الأهم من ذلك أنّنا يجب أن ندعم الرقابة الشرعيّة، ونبحث عن طرق تمكن المؤسّسات الحكوميّة من ممارستها من دون أن تنتهك الخصوصيّة، وتخرّب الأمن، وتتعدّى على حق المواطن في التحرّر من الترصّد والاشتباه المفرط. إذا استطعنا إعطاء قوى إنفاذ القانون طرقاً جديدة للتحقيق في الجرائم، فسيكفّون عن المطالبة بتهديم الأمن لمصلحتهم.

لن تختفي الصراعات الجغرافيّة- السياسيّة، وتشكّل الاستخبارات الخارجيّة أداة متفرّدة في مواجهة تلك الحوادث[28]. وفيما أكتب هذه الكلمات في صيف 2014، تحشد روسيا قوّاتها ضد أوكرانيا، وتتنمّر الصين على اليابان وكوريا في بحر الصين الجنوبي، ويقدِم إرهابيّو الـ «إيغور» على قتل صينيّين من شعب الـ «هان»، وتهاجم إسرائيل غزّة، وتساعد قطر وتركيا غزّة للدفاع عن نفسها، وتتخبّط أفغانستان في متاهتها، وتتفتت ليبيا، وتعود مصر إلى الديكتاتوريّة، وربما تعاود إيران برنامجها النووي، ويجتاح فيروس «إيبولا» غرب أفريقيا، وتختبر كوريا الشماليّة صواريخ جديدة، وتقتل سوريا شعبها، ويهيمن على أجزاء كبيرة من العراق منظّمة تنتمي اسميّاً إلى التطرّف الإسلامي وهي تعرف باسم «الدولة الإسلاميّة في العراق والشام». وليس ما سبق سوى ما يرد في نشرات الأخبار. وعندما تقرأ هذا الكتاب، ستكون القائمة مختلفة، لكنها لن تكون أقل فداحة. وأؤكّد لك أن أحداً في البيت

الأبيض لن يدعو «وكالة الأمن القومي» إلى تقليص عملياتها في جمع المعلومات عن تلك التهديدات وما يشبهها. ويجب عليهم ألا يفعلوا.

إضافـة إلى ذلـك، يتملـك حكومات العالم ذعر واسـع من إمكان شـنّ هجمات في الفضـاء السـبراني. يـأتي معظم ذلك الذعر مـن ردّ فعل مبالغ فيـه، لكن المخاطر حقيقيّة. ويتخبّط الدفاع السبراني في مشكلة العمل الجماعي التقليديّة. إذ تدير أيدي القطاع الخاص معظم البنية التحتيّة للفضاء السـبراني، لكن معظم الضرر الذي ربما ينجـم من هجمات سـبرانيّة كبرى، سـيحيق بالجمهـور ككل. ويعني ذلـك أنّه على المدى الطويل سـيصعب الركون إلى الشركات التي تدير بنيتنا التحتيّة، لتقديم حماية مناسبة لتلك البنية. ثمة ضرورة لنوع من التدخّل الحكومي. في 2013، صرّح مدير «وكالة الأمن القومي» الجنرال كيث ألكسندر بالقول: «لا أستطيع الدفاع عن البلاد ما لم أدخل الشبكات كلّها»[29]. وتعبّر تلك الكلمات عن الرأي السائد في واشنطن.

نعم، يجب علينا الحسـم بشـأن المدى الذي نرغب فيه بوجود الوكالة في شـبكاتنا كلهـا. لكـن، يجب أيضاً أن نسـاعد الوكالـة في ألا تطلب الدخول إلى شـبكاتنا كلها. إذا اسـتطعنا أن نقدّم للحكومات طرقاً جديدة في الحصول على معلومات عن الدول العدوانيّة، والمجموعات الإرهابيّة وعناصر الإجرام العالمي؛ فلسوف تقلّ حاجتها إلى الإجراءات المشتطة التي وصفتها في هذا الكتاب. إنّها دعوة أصيلة إلى أفكار وأدوات وتقنيّـات جديـدة. بكل صـدق، لا أعرف كيف سـتكون الحلول. ثمة طريق وسـط، ومنـوط بنـا جميعاً أن نعثر عليه. إذا أردنا من مؤسّسـات كـ «وكالة الأمن القومي» أن تحمي خصوصيّتنا، يجب علينا أن نعطيها طُرُقاً جديدة لأداء عملها الاستخباراتي.

اختر حلفاءك وأعداءك

تستند قوانيننا إلى الموقع الجغرافي. ولفترات طويلة من التاريخ البشري، بدا ذلك الأمـر منطقيّاً تماماً. ويبدو ذلك أقل منطقيّة عندما يتعلّق الأمر بالإنترنت؛ لأن تلك الشبكة دوليّة جداً.

مـن الواضـح أنّك تخضع للقوانـين الشرعيّة للبلد الذي تعيـش فيه، لكن عندما تكون على الشـبكة، تضحي الأشـياء أكثـر تعقيداً. إذ إنّك تتأثّـر بقوانين البلد الذي يعيـش فيه صُنّـاع المكوّنات الإلكترونيّـة، وقوانين البلد الذي يسـتقر فيه الشركات التـي تبيـع البرامـج، والبلـد الـذي يقـدّم لك خدمة «حوسـبة السـحاب» بشـبكة الإنترنـت. وسـوف تتأثّـر أيضاً بقوانـين البلد الذي تسـتقر فيه الخـوادم التي تختزن معلوماتـك وبياناتك، وقوانين البلـدان التي تمرّ فيها بياناتك عندما تتحرك بخطوط الإنترنت[30].

مثلاً، يجبر «قانون باتريوت» الشركات الأميركيّة على تسليم بيانات إلى الحكومة الأميركيّـة عندما تطلبهـا، بغض النظر عن مكان تخزينها. ربما تكون مواطناً فرنسـيّاً يعيش في فرنسـا، وتخزّن «مايكروسـوفت» بريدك الإلكتروني في خوادمها في أيرلندا حصريّـاً. ولكن، لأنّ «مايكروسـوفت» شركة أميركيّة، تزعـم الولايات المتّحدة أن تلك الشركة مجبرة على تقديم بياناتك لها عند الضرورة[31]. وترغب المملكة المتّحدة في امتلاك نفاذ مماثل[32].

ويعنـي ذلك أنّه يجب عليك أن تختار أي البلدان تثق بها، وما هي الشركات التي تثق بها.

لا تتسـاوى الشركات كلها في السـوء. تسـتطيع الحصول على البريد الإلكتروني والمفكرة ودليل العناوين، إما من «غوغل» أو «آبل». سوف تحمي الشركات بياناتك مـن الجمع الجماعي في بلدان كثيرة، لكنهما ستسـلّمانها لحكومـات عـدّة إذا أجبرتا قانونيّاً على ذلك. ينخرط «غوغل» راهناً في مشروع ضخم لحماية بيانات مستخدميه من رقابة الحكومة. في المقابل، يجمع «غوغل» بيانات الجمهور ويسـتخدمها لغايات الإعلان، فيما تستند «آبل» إلى نموذج عمل مغاير يحمي خصوصيّة مستخدميها[33].

هل تثق بشركة في الولايات المتّحدة لا قيود عليها في ما تسـتطيع عمله ببياناتك، إضافـة إلى خضوعها لطلبات قانونيّة من الـ «إف بي آي» و«وكالة الأمن القومي»،

بخصوص تلك البيانات؟[34] أم تثق بشركة أوروبيّة تعمل ضمن قيود حكوميّة صارمة بشأن رقابة الشركات، لكنها تخضع لرقابة بلا قيود تمارسها حكومة بلدها والولايات المتّحدة معاً، ما يعني أن بياناتك تعبر الحدود الدوليّة؟ إذا لم تشتر من شركة «سيسكو سيستمز» معدّات تشبيك بسبب تخوّفك من «الأبواب الخلفيّة» لـ «وكالة الأمن القومي»، فمن أين ستشتري معدّاتك؟ هل تلجأ إلى «هواوي» الصينيّة؟ تذكّر التشبيه الذي أوردته في الفصل 4 عن الإقطاعيّة في العلاقة بين الجمهور والشركات؛ أي السادة الإقطاعيّين تثق به أكثر؟

يصعب تحديد نقطة البداية. ففي عالم «حوسبة السحاب» حاضراً، لا نعرف أي الشركات تستضيف معلوماتنا فعليّاً. إن شركة إنترنت كـ «أوربتز» (Orbitz) تملك بنيّة تحتيّة تستضيفها خوادم شركة «آتلاسيان» (Atlassian) التي تحصل على بنيتها التحتيّة من مقدّم خدمات إنترنت كـ«راك سبايس» (Rack- Space)؟ فهل لك أن تعرف أين تكون فعليّاً بياناتك المخزّنة لدى «أوربتز»؟

يجب أن نمتلك القدرة على معرفة أين تخزّن بياناتنا ومعلوماتنا فعليّاً، وتعيين البلد الذي نرغب في تخزين معلوماتنا فيه، والبلد الذي لا نرغب في أن تكون بياناتنا قريبة منه. في الوقت عينه، يجب أن نبذل قصارى جهدنا. وفي معظم الأحيان، يجب أن نعترف ببساطة أننا لا نعرف.

لكن، عندما يتعلق الأمر بالحكومات، أنا مضطر للقول بأسف إنني أفضل أن تتجسّس عليّ حكومة الولايات المتّحدة، أكثر من أي نظام آخر.

حرّض على التغيير السياسي

في العام 2014، ألغت «محكمة العدل الأوروبيّة» قوانين الاتحاد الأوروبي المتعلّقة بتخزين البيانات، وكانت تفرض على مقدّمي خدمات الإنترنت الاحتفاظ بالبريد الإلكتروني والبيانات عن المكالمات الهاتفيّة، لمدة سنتين[35]. في ردة فعل،

سارعت الحكومة البريطانيّة إلى إقرار قانون جديد أعاد فرض تلك المدّة على تخزين المعلومات، كما أعطيت الشرطة صلاحيات جديدة في رقابة المواطنين[36]. بدا ذلك قيداً سياسياً كريهاً، لكن المثير هو الطريقة التي برّر بها رئيس الوزراء البريطاني ديفيد كاميرون ذلك القانون في أحد برامج الراديو[37]. إذ قال: «ببساطة، لست مستعدّاً لأن أكون رئيس الوزراء الذي يتحدّث إلى الناس بعد ضربة إرهاب مبيّناً لهم أنه كان بوسعنا فعل المزيد في الحيلولة دونها».

لا يعدو ذلك كونه خطاب الخوف، لكنه ليس خوفاً من الإرهابيّين. إنّه الخوف السياسي من تحمّل الملامة إذا حدثت ضربة إرهاب. يرغب السياسيّون في فعل أي شيء بغض النظر عن كلفته وقدرته فعليّاً على جعل الناس أكثر أمناً، وآثاره الجانبيّة؛ كي يتجنّبوا الملامة عن كونهم لم يبذلوا جهداً أكبر. يفسّر ذلك الخوف معظم السياسة التي انتُهِجَت بعد 9/ 11، وغالبية برامج الرقابة العامة التي مارستها «وكالة الأمن القومي». يتملك سياسيّونا الرعب من ملامتنا لهم بأنهم لم يفعلوا كل ما قالت وكالات الاستخبارات أنه واجب على السياسيّين فعله لتجنّب مزيد من الإرهاب.

يجب علينا إقناعه وبقية مواطنينا الناخبين، بأنه يتعين عليه فعل الأمر الصحيح مهما كان شأنه.

معظم الحلول التي عُرِضَت في الفصلين السابقين تتطلّب من الحكومات إما تفعيل القوانين السارية أو تغيير القانون. وإلى حدّ كبير، لن يحدث أيّ من الأمرين ما لم نطالب بذلك. يتردّد السياسيّون في خوض تلك النقاشات، ويتردّدون أكثر في تفعيل قيود مجدية على رقابة الحكومة. وبطبعهم، يبدي المشرّعون احتراماً خاصاً لطلبات قوى إنفاذ القانون، ويوظّف المجمّع الصناعي- الرقابي مجموعات ضغط لمؤازرتهم. لا يرغب أحد في الظهور بمظهر الضعيف حيال الجريمة والإرهاب. وحاضراً، عندما ضبطت وكالات الاستخبارات الأميركيّة أثناء تجاوزها القانون، لا يتهدّد السجن أحداً سوى من أطلقوا صافرات الإنذار حيال ذلك.

مـن جهة الـشركات، تبذل مجموعات الضغط السـياسي قصارى جهدها لضمان عـدم حـدوث إصلاح جـدي بشـأن الرقابة التي تمارسـها الـشركات. ترفـع حريّة السـوق مبرّراً لاسـتمرار ذلك الشـلل. وكذلك تضغط قوى الأمن وأجهزة الأمن القومي كي تضمن بقاء بياناتنا في متناول أيديها.

إذا أردنا أن يصوّت مشرّعونا ضد المصالح القويّة للعسـكر وقوى إنفاذ القانون والشركات المثقلة بمجموعات الضغط (سـواء التي تمـّد الحكومة بالبيانات أم تلك التي تتجسّس علينا مباشرة)؛ يجب أن نجعل من أنفسنا أقوياء. ويعني ذلك أنه يجب علينا الانخراط في العملية السياسيّة. ولديّ في ذلك 3 توصيّات محدّدة.

لاحـظ وجـود الرقابـة. إنّهـا الخطـوة الأولى. لا يتبدى معظـم الرقابـة للأعين، لكنـه ليس خفيّـاً كليّاً. ربما كانت الكاميرات صغيرة، لكنك تسـتطيع ملاحظتها إذا حدّقت. تسـتطيع أن تلاحظ مَنْ يقوم بالمسـح الضوئي لبطاقة هويتك عندما تدخل المقصف. تسـتطيع وضع مكـوّن داخلي في متصفحك كي تعـرف من يلاحقك على الإنترنـت. بإمكانـك التنبّه للأخبار عـن الرقابة. هناك مواقع عـلى الإنترنت تعرف بكاميرات المراقبة[38]. كلما عرفت أكثر، يتحسّن فهمك لمجريات الأمور.

تحـّدث عن الرقابة. إنّها الخطوة الثانيـة. كلما زاد حديثنا عن الرقابة، ازداد الناس إدراكاً بمجرياتهـا. وكلـما ازداد ذلك الإدراك، يصبح الناس أكثـر اهتماماً بها. وكلما تحدّثنا عن الرقابة علانية، يدرك مشرّعونا أكثر أننا نهتم لأمرها.

أقصـد ذلـك بصورة عامـة تماماً. تحـدّث عـن الرقابـة إلى عائلتـك وأصدقائك وزملائـك. لا تكن من أولئك المزعجين الذيـن لا يضعون تدوينات إلا عنها، لكن تشـارك بما يرد في الأخبار عنها بوسـائط الـ «سوشال ميديا». انضم إلى التجمّعات، ووقّع على البيانات العامة بصددها. اكتب إلى ممثلك في البرلمان. أعطِ نسخاً من هذا الكتاب إلى أصدقاء كهدايا. لتكن آراؤك معروفة. إنّها أشياء مهمّة.

تحـّدث عن القوانين في بلادك. ما هي أنـواع الرقابة المشروعة في موطنك؟ كيف تتدخّـل مصالح رجال الأعمال فيها، وما هو نـوع الرقابة المتاحة لهم قانونيّاً؟ ما هي الحقوق التي يملكها الناس في استخدام أدوات تمكين الخصوصيّة؟ ابحث عنها.

تتمثّل إحدى المناحي الأكثر سورياليّة التي أظهرتها كشوفات سنودن عن «وكالة الأمـن القومـي»، في أنها جعلت نظريات المؤامـرة الأكثر انغماسـاً في البارانويا تبدو كأنها نص متماسك من العقلانيّة والحسّ السديد. من السهل نسيان تلك التفاصيل، والعـودة إلى الإحســاس بالرضى؛ لذا فإنّ اسـتمرار النقاش عن تلـك التفاصيل هو وحده الكفيل بالحيلولة دون ذلك.

تنظّم سياسـيّاً. إنّها استراتيجيّتنا الأشد فعاليّة. ثمة أمثلة حديثة عن كيفيّة انتظام الناس سياسـيّاً ضد الرقابة. ففي كوريا الجنوبيّة، احتجّ الأسـاتذة على وضع قواعد بيانات جديدة عن الطلبة[39]. واحتجّ المسـتهلكون الألمان على وضع عربات مزوّدة بنظام «رفيد» تمسـح البضائع والأقسـام والرفـوف التي يمرّون بهـا أثناء تجوالهم في المخازن الكبرى[40]. كما احتج مسـتخدمو «فيسـبوك» على فرض شروط استخدام جديـدة في صفحاتهـم[41]. واحتجّ مسـافرون مـع شركات الطـيران الأميركيّة على اسـتعمال ماسـحات ضوئيّة تصور الجسـد بأكمله[42]. لا تتكلّل حملات الاحتجاج بالنجاح دوماً، كما أن نتائجها بعيدة عن الكمال، لكن من النافل الإشـارة إلى الأهمية التـي يكتسـبها التحرّك جماعيّاً. يجب أن نعي بأن تلـك الأمور تطالنا جميعاً، وحلولها تكون عامة أيضاً.

ليس هذا بكتاب عن كيفيّة التنظّم سياسيّاً، وهناك أشخاص أكثر تمرّساً مني بكثير في شرح كيفيّة تحريك التغيير السياسي. أعرف أن السياسات هي أمور لا تحصل أثناء الانتخابات وحدها. بالأحرى، إنّها عملية مستمرة، وتشمل الانخراط مع المشرّعين، والاحتجـاج علنـاً، وتقديم الدعم لمجموعات لا تسـعى إلى الربح وتنشـط في ذلك المجال. انظر إلى «مؤسّسة الحدود الإلكترونيّة» (Electronic Frontier Foundation)

و«مركـز معلومـات الخصوصيّـة الإلكترونيّـة» (Electronic Privacy Information Center) و«مركز الديمقراطيّة والتكنولوجيا» (Center for Democracy & Technology) و«المنظّمـة الدوليّـة للخصوصيّـة» (Privacy International) و«معهـد التكنولوجيا المفتوحة» (Open Technology Institute) وغيرها. تكافح تلك المجموعات كلّها من أجل رقابة أقل وخصوصيّة أكثر. ادعمها.

لا نسـتطيع فعل الكثير في بقية أرجاء العالم [أي خارج الولايات المتّحدة]، لكننا نسـتطيع أن ندفع باتّجاه التغيير حيثما نقدر على ذلك. بعدها، نسـتطيع التحرّك ببطء نحو الخارج. هكذا يحدث التغيير عالميّاً[43].

لا تستسـلم. القدريّـة عـدوّة التغيـير. تتبدّى القدريـة في القول بـأن الحكومات والـشركات الكبرى تملكان أسـباب القوة كلها، ومعظم السياسـيّين ليسـت لديهم الرغبة في تقييدهما؛ ما يعني أننا عاجزون عن تغيير الأشياء. وكذلك تتبدى القدريّة في القول إن الرقابة الشـاملة هي كليّة القدرة إلى حدّ أننا لا نستطيع مقاومتها، بل إن من شأن المقاومة أن تضعنا قيد اهتمامها على كل حال.

تحمل تلك التأكيدات شيئاً من الحقيقة، لكن خلاصاتها مغلوطة. فمن شأن الأمن الجيّد للكومبيوتر والانتشـار الواسـع للتشـفير، تصعيب مهمة الرقابة العامة. ومن شـأن العمل على التعاون انتقائيّاً مع الشركات على أساس سياساتها في الخصوصيّة؛ جعل الشركات أكثر ميلاً للسياسـات الحسـنة بصدد الخصوصيّة. وبمرور الوقت، سـيخفت افتتاننـا بـ«البيانـات الضخمة» وخوفنا غـير المعقلن مـن الإرهاب. وفي نهايـة الأمر، سـوف تعمـل القوانين على تقييد سـلطة الحكومة والـشركات معاً على الإنترنت.

يمثّل ما أوصي به نقلات كبرى سياسـيّاً، تسـتلزم بذل كثير من الجهد. وتاريخيّاً، عُدَّت النقلات السياسيّة الكبرى عبثيّة في بداياتها. تلك هي طريقتها. يجب أن نقاتل

من أجل التغيير السياسي، ونستمر في القتال حتى ننتصر. وحتى ذلك الحين، هنالك كثير من المعارك الصغيرة التي يجب أن نكسبها.

هنـاك قـوة في الكثـرة، فـإذا تصاعـد صـوت الجمهور، سـوف تُجـبَر الشركات والحكومات على الاستجابة له. ما نحاوله هو منع ظهور حكومة شموليّة من النوع الـذي رسـمته رواية جورج أورويـل 1984، وكذلك الحيلولة دون سـلطة تديرها الشركات، على غرار ما رسـمته مجموعة كبيرة من روايات الخيال العلمي المتشـائمة المنتمية إلى ثقافة الـ «بانك السبراني»(*) (Cyberpunk).

وبـأي حال مـن الأحوال، لسـنا قريبين مـن النهايتـين، لكن القطـار يتحرّك في اتّجاههما معاً، ويجب علينا تشغيل المكابح.

(*) ظهـرت حركة الـ"بانك" الشـبابيّة المتمـرّدة في ثمانينيات القرن العشرين، خصوصـاً في بريطانيا أيام رئيسـة الـوزراء الراحلـة مارغريت تاتشر. كانوا متشـائمين بمسـار المجتمعـات الغربيّـة وثقافاتها. واشـتهروا بقصّات الشعر التي تشبه عُرف الديك، والأوشام الكثيرة على الجسد، ووضع الغرسات المعدنيّـة في الأنوف، والموسـيقى التي تمزج الصخب بالكآبة. لاحقاً، صـار كثير من الـ"بانك" روّاداً مؤسّسين في المعلوماتيّة في أميركا، وحملوا شيئاً كثيراً من ثقافة التمرّد إليها.

16

الأعراف الاجتماعيّة ومقايضة «البيانات الضخمة»

في الفصول الثلاثة السابقة، تحدّثت عن الحاجة إلى إجراء تغييرات كثيرة: في الحكومة والشركات والسلوك الفردي. كان بعض التغييرات تقنيّاً، لكن معظمها يتطلّب قوانين جديدة أو على الأقل سياسات جديدة. في هذا الوقت، يبدو معظمها غير واقعي، على الأقل في الولايات المتّحدة. إذ أعيش في بلد ما زالت غالبية السكان فيه لا تطالب بتلك التغييرات، إضافة إلى أنّ ذلك البلد لا تترجم فيه إرادة الناس بسهولة إلى أفعال تشريعيّة.

تبدو غالبية الناس [في الولايات المتّحدة] غير مبالية بأن تجمع الشركات تفاصيلها الحميمة وتستخدمها أيضاً، معتقدة بأن الرقابة التي تمارسها حكومات يثقون بها تمثّل شرطاً أساسيّاً لحفظ أمنهم. ما زال معظم الناس يخاف الإرهاب بشكل مبالغ فيه. ولا يفهم الناس المدى الذي بلغته قدرات الرقابة عند الحكومة والجهات الخاصة. ويقلّلون من شأن الرقابة الجارية، غير مدركين أن الرقابة الحكوميّة العامة لا تحفظ أمن غالبيتنا. ويبدو معظم الناس مرتاحاً إلى مقايضة بياناته الحسّاسة بالحصول على بريد إلكتروني ومحرّك بحث على الإنترنت أو منصّة للثرثرة مع أصدقائه.

يختلف الوضع في أوروبا إلى حدّ ما؛ لأنّها تفرض قوانين أشد صرامة على الشركات وتمارس حكوماتها رقابة أقل، لكن مشاعر عامة الناس تتشابه مع ما في الولايات المتّحدة إلى حدّ كبير.

قبل أن نتوصل إلى تغيير سياسي، يفترض ببعضٍ من قيمنا الاجتماعيّة أن تتغيّر. يجب أن نصل إلى نقطة يدرك الناس فيها المدى الفائق الاتّساع للرقابة، وما يولّده ذلك من تمركز فائق للقوة والسلطة. عندما يفعلون ذلك، ربما قال معظم الناس: «ذلك الأمر ليس سلبياً». يجب أن نستجمع القوة السياسيّة لنقارع قوى إنفاذ القانون ووكالات الاستخبارات القوميّة من جانب الحكومة، وكذلك المتعاقدين مع الحكومة وصناعة الرقابة من جهة الشركات. وقبل حدوث أيٍّ من الأمرين، يجب إحداث تغييرات كبرى في طريقة نظر المجتمع للخصوصيّة وكيفيّة تقييمه للخصوصيّة والأمن والحريّة والثقة، إضافة إلى حفنة من المفاهيم المجرّدة التي تحدّد ذلك النقاش.

إنّه لأمر صعب. إذ تميل المشاعر السياسيّة إلى التحرّك باتّجاه الممارسة العمليّة. نحن ماهرون في قبول الأمر القائم، أيّاً كان ومهما كانت جدّته. (للأمانة، يطيح بعقلي أن كل تلك الرقابة ظهرت في أقل من عقدين). بتنا ننمو في ظل تعوّدنا على الـ «بان أوبتكون»(*). بوسعك أن تراه يتضخّم باستمرار فيها الناس يهزّون أكتافهم قائلين: «ما الذي تنوي فعله»؟ بوسعك أن تراه على المستوى الصغير في كل مرّة يعمد فيها «فيسبوك» إلى الانحدار بمستوى الخصوصيّة عند مستخدميه: في البداية يتذمّر الناس، وسرعان ما يعتادونه.

تتناول بقية هذا الفصل كل التغيّرات اللازمة في السلوك. هناك طُرُق يجب اتّباعها لتعديل مشاعرنا وأفكارنا، إذا قيّض لنا الخروج من آسار مجتمع الرقابة.

(*) انظر الفصل 2.

إعادة صوغ معايير خوفنا

وُقّع «قانون باتريوت» في 26 تشرين أول (أكتوبر) 2001، بعد 45 يوماً من هجمات الإرهاب ضد البنتاغون ومركزي التجارة العالميين. لم يكن سوى «قائمة أمنيات» الشرطة والسلطات وقوى الاستخبارات، ومُرّر بأغلبية ساحقة في مجلسي النوّاب والشيوخ، وبحد أدنى من النقاش. لم يقرأه أحد في الكونغرس قبل التصويت عليه[1]. وتقريباً، كان كل الناس راغبين في إقراره، على الرغم من عدم فهم إملاءاته[2].

في 2014، حضرت نقاشاً تحدّث فيه تيم دافي، الرئيس والمدير التنفيذي لوكالة الإعلانات «إم إند سي ساتشي» (M & C Saatchi)، وحاول فيه تقديم رسالة محسّنة عن الخصوصيّة[3]. وسأل: «أين ترسم خط الفصل؟» في محاولة لرسم صيغة عن الخصوصيّة. لكن، إذا كان المستمعون في ذعر من الإرهابيّين، فلسوف يرسمون الخطوط بما يسمح بالكثير جداً من الرقابة[4]. وأشار جاك غولد سميث أستاذ القانون في «جامعة هارفرد»، إلى أنّه عندما نكون مذعورين، تؤدّي زيادة إشراف الكونغرس إلى إعطاء مزيد من الصلاحيّة إلى «وكالة الأمن القومي»[5].

يتقدّم الخوف على الخصوصيّة[6]. يتقدّم الخوف من الإرهاب على الخوف من الطغيان. إذا بلغ من القوة مبلغاً كافياً، فلسوف يتقدّم على الحجج التي جمعها الكتاب كافة[7]. بالنسبة للناس، إنّه الخوف من ضربة الإرهاب المقبلة. بالنسبة للسياسيّين يكون الأمر كذلك، إضافة إلى الخوف من تلقي *الملامة* عن ضربة الإرهاب التالية. لكنه الخوف، في كل الأحوال. لنتذكّر حديث رئيس الوزراء كاميرون الذي ورد في الفصل السابق. إنّه ما أسمعه مراراً وتكراراً من مسؤولين حكوميّين عندما أسألهم عن وضوح انعدام فعاليّة الرقابة العامة في مواجهة خطر الإرهاب. وإذ يقرّون بذلك، إلا إنّهم يرون في الرقابة العامة سياسة ضمان. ويعرفون أن جهودهم في الرقابة الموجّهة سوف تفشل عند نقطة ما، ويعقدون الأمل على أن تكون الرقابة

العامـة حـاضرة كاحتياط. يصح القول حقاً إن الاحتـمالات ضئيلة بأن تكون فعّالة على ذلك النحو، لكنهم [المسؤولين الحكوميين] يعتقدون بأنه يجب عليهم فعل كل شيء ممكن، من أجل أمن البلد وأمن مناصبهم معاً[8].

ويغـض النظـر عن مدى الخطر، لا تمثّـل الرقابة العامة إجراءً مضـاداً فعّالاً؛ فيما تتسـم بالفعاليّة عمليات الاستخبارات وإجراءات الشرطة. يجدر بنا مقاومة النزعة إلى *القيام بشيء ما*، بغض النظر عما إذا كان العمل المقترح فعّالاً أم لا.

يمثّـل الإبقـاء على الخـوف متأجّجاً تجـارة هائلـة[9]. يعرف العاملـون في مجتمع الاسـتخبارات أنّـه أسـاس نفوذهـم وقوّتهم. ويعلـم المتعاقـدون مع الحكومـة أنّه مصدر الأموال لعقودهم. ولاحظ الكاتب والناشـط على الإنترنت كلاي شـيركي أنّ «المؤسّسـات سـتحاول الحفاظ على المشـكلة التـي تمثّل [تلك المؤسّسـات] حلاً لها»[10]. الخوف هو تلك المشكلة.

إنه الخوف الذي تؤجّجه نشرات الأخبار يوميّاً. وبمجرد حدوث جريمة مرعبة أو هجوم إرهابي يفترض أنه كان ممكناً منعه بمجرد إعطاء الـ «إف بي آي» أو «وزارة الأمـن الوطنـي» نفاذاً أكـبر إلى بعض المعلومات المخزّنة في «فيسـبوك» أو المشـفّرة في «آي فـون»؛ يضحـي مطلب الناس هـو أن يعرفوا لماذا لم تحصـل الـ «إف بي آي» أو «وزارة الأمـن الوطني» عـلى حق النفاذ إلى تلك المعلومـات، ولماذا جرى منعهم مـن «الوصـل بين النقط». وعندها، تتغـيّر القوانين كي تعطيهم مزيداً من السـلطة. وبالعـودة إلى جـاك غولد سـميث، فإنّـه يقول: «سـتزيد الحكومة من سـلطاتها كي تستطيع ملافاة التهديد للأمن الوطني (لأن الناس يريدون ذلك)»[11].

نحتـاج إلى طريقـة أفضل في التعامل مع ردود أفعالنـا العاطفيّة حيال الإرهاب، تكون غير إعطاء حكومتنا شيكاً على بياض في التعدّي على حريّاتنا، في محاولة يائسة لاسـتعادة الشـعور بالأمن. إذا لم نعثر على أي طريقة لفعـل ذلك، فعندها يمكن أن يقـال إن الإرهـاب حقّـق نجاحاً حقيقيـاً. أحد أهـداف الحكومة هـو إعطاء الأمن

لشعبها، لكن في الديمقراطيّات، يجب علينا خوض المخاطر[12]. عندما يرفض المجتمع المخاطرة- في الجريمة والإرهاب وغيرهما- يكون دولة بوليسيّة بالتعريف. وتحمل الدولة البوليسيّة مخاطرها الخاصة أيضاً.

لا ينحى باللائمة على السياسيّين وحدهم في ذلك[13]. الإعلام العام مُدانٌ أيضاً. وبتركيزه على الحوادث النادرة والمشهديّة، يولّد الإعلام لدينا رد فعل شرطي للتصرّف كأنما الإرهاب شيء شائع أكثر مما هو عليه فعليّاً، ولخشيته بأكثر من نسبة حدوثه فعليّاً. وكذلك نُلام نحن أيضاً، إذا اشترينا البروباغندا التي يبيعنا إياها الإعلام.

علينا أيضاً أن نعارض مفهوماً مفاده أنّ التكنولوجيا الحديثة تجعل الأشياء كلها مختلفة[14]. في الأيام والأسابيع التي تلت هجمات الإرهاب في 9/ 11، عندما خضنا في نقاش عن قوانين جديدة وسلطات جديدة للأمن؛ سمعنا العبارة التالية: «الدستور ليس حلفاً انتحاريّاً». إنّها تعبّر عن مشاعر منغمسة في الخوف، ويجدر تبيان معناها[15]. يشبه ما تقوله تلك العبارة ما يلي: «الناس الذين كتبوا قوانيننا لم يكن لهم أن يتوقّعوا الوضع الذي نواجهه الآن. لذا، فإن القيود التي فرضوها على سلطات الشرطة وقوى الأمن، والنواهي التي فعّلوها ضد الرقابة، لا تنطبق علينا. إنّ وضعنا متفرّد، وعلينا تجاهل تلك الأمور كلّها». تمثّل السبب الرئيس في استسلامنا لتلك المفاهيم في اعتقادنا بأن الضرر الذي يستطيع الإرهابيّون التسبّب به، هو من الضخامة بما يجعل من غير المفهوم أن نركن إلى الوسائل التقليديّة في إنفاذ القانون، والمحاكمات المبنيّة على الوقائع.

إنّ ذلك ليس صحيحاً أبداً. إنّها مغالطة نفسيّة شائعة الاعتقاد بأننا نعيش أوقاتاً فائقة الفرادة، وأنّ تحدّياتنا لا تشبه ما قبلها إطلاقاً، ما يوجب تجاهل الضوابط الاجتماعيّة التي وضعناها قبلاً للحدّ من قوة السلطات الحكوميّة. استسلم الرئيس إبراهام لينكولن لتلك المغالطة عندما أوقف العمل بإصدار مذكرة قانونيّة كشرط

لمثول شـخص ما أمام المحكمة، أثناء الحرب الأهليّة. وتكرّر الأمر عينه مع الرئيس وودرو ويلسـون عندما اعتقل ورحّل قادة العمّال والاشتراكيّين بعيد الحرب العالمية الأولى مباشرة. وفعل الرئيس فرانكلين روزفلت الأمر عينه عندما احتجز أميركيّين من أصول يابانيّة وألمانيّة وإيطاليّة، أثناء الحرب العالمية الثانية. وكرّرنا ذلك في الحقبة المكارثيّة أثناء الحرب الباردة. وها نحن نفعلها كرّة أخرى بعد 9/ 11.

لا يشـكّل الخوف طريقاً وحيداً للرد على تلك التهديدات، وهناك حالات كثيرة لم تتخـل فيها المجتمعات عن حقوقها، في سـياق سـعيها إلى البقـاء آمنة. ففي خضم المجـزرة المروّعـة في النرويج التي ارتكبهـا أندرياس بريفيك، حافظـت تلك البلاد إلى حـد كبير على قيمها الأساسـيّة في الحريّة والانفتاح[16]. وهناك الجملة الشـهيرة للرئيس فرانكلين دوايت روزفلت نفسه: «الشيء الوحيد الذي يجب أن نخاف منه، هو الخوف نفسه». أن لا ننهزم، هو رد الفعل الصحيح على الإرهاب[17].

ثمـة أمل للولايـات المتّحدة[18]. لم يكن الخوف رد فعلنـا دائماً على الإرهاب. وباسـترجاع التاريـخ الحديـث، فـإن الرؤسـاء الذين قاومـوا الإرهـاب- ترومان، آيزنهـاور، نيكسـون، وريغان أحيانـاً، وبوش الأب- حقّقوا نتائج عمليّة وسياسـيّة أفضـل مـن أولئـك الذين اتّخـذوا الإرهـاب ذريعة للحصـول على مظلّة سياسـيّة: كارتـر، ريغـان (معظم الوقت)، وبـوش الابن. نحتاج إلى الإقرار بقوة السياسـيّين الذيـن يحمون حريّاتنا أثناء المخاطر، وضعف السياسـيّين الذيـن يعجزون عن حلّ المشـاكل فيختـارون التضحيـة بحريّاتنـا. بعد ما يزيـد على عقد مـن 9/ 11، أزف الوقـت للتحرّك بعيـداً من الخوف، ونعـود إلى القيم الأميركيّة الأساسـيّة في الحرية والتحـرّر والعدالـة[19]. وثمة مؤشّرات على أننا نفعل ذلك. ففي 2013، شرعنا في رؤيـة انزياح لافت في مدركات الأميركيّـين عن قبول مبادلة الحريّات المدنيّة بالأمن القومي[20].

إعادة صوغ معايير الخصوصيّة

تتسم تعريفاتنا الشخصيّة للخصوصيّة بأنها ثقافيّة وظرفيّة في آن معاً. إذ كانت مختلفة قبل 100 سنة عن حالها حاضراً، ولسوف تكون مختلفة أيضاً بعد 100 سنة من الآن. وتختلف في الولايات المتّحدة عما هي عليه في أوروبا واليابان وأمكنة أخرى[21]. كما أنها تتفاوت بين الأجيال.

وحاضراً، تؤثّر الإنترنت في توجّهاتنا حيال الخصوصيّة، بطريقة غير مسبوقة. ويرجع ذلك إلى أن الطرق الرئيسة التي نستخدمها تتمثّل في التعلّم من بعضنا بعضاً. إذ يتصيّد المحامون المحلّفين المحتملين، ويتتبع الباحثون عن وظيفة المدراء التنفيذيين، وتترصد أقسام الموارد البشرية في الشركة بالمتقدمين إلى الوظائف[22]. قبل المواعدة الأولى، يتربص الناس ببعضهم بعضاً[23]. حتى إن ذلك الشيء له اسم: قسم التربّص في محرّك البحث «غوغل»[24].

على خطوط الإنترنت، نسبر غور الأشياء باستمرار، وأحياناً يتعدّى أحدنا على خصوصيّة الآخر. يمكن ألا يكون ذلك مريحاً أبداً. تعطي الطبيعة شبه الأبديّة للاتّصالات على الإنترنت فرصاً من الأنواع كافة لمن يريد أن يضايقك. وبسهولة، يمكن تحويل رسائل الـ «إيميل» التي أرسلتها إلى أحدهم بصورة شخصيّة، كي تصبح في متناول آخرين. وباستمرار، يفعل الأطفال حاضراً ذلك الأمر ببعضهم بعضاً. إذ يحوّلون لبعضهم بعضاً المحادثات الخاصة والصور والرسائل، أو يظهرون التدوينات التي كتبت بصورة شخصيّة على مواقع الـ «سوشال ميديا». ومن أسباب إقبال الشباب والمراهقين على التطبيقات الرقميّة التي تسمح بحذف الرسائل والصور بعد ثوانٍ قليلة من عرضها، هو أنها تسمح بتجنّب تلك الأوضاع. في المقابل، تنحو الصفحات القديمة على الـ «ويب» للبقاء، بطريقة أو أخرى. في 2010، جرى التنقيب على بروفايل المواعدة «أوكي كيوبيد» العائد إلى مؤسّس موقع «ويكيليكس» جوليان أسانج، ووُضِع قيد النقاش العام[25].

لعل الأسوأ هم الناس الذين يستخدمون الإنترنت للتحرّش والإذلال. تعطي «أشرطة الانتقام الإباحي»- والقسم الأكبر منها هو شاب ينشر صوراً عن ممارسة جنسيّة متفلتة مع صديقته السابقة- نموذجاً متطرّفاً عن ذلك[26]. جعلت مواقع نشر الصور التي تلتقطها الشرطة عند اعتقالها شخصاً ما، من ذلك المنحى تجارة كاملة قوامها الابتزاز[27]. تعدُّ تلك الصور جزءاً من السجلات العامة، لكنها لا تكون متاحة بيسر. ويقتنص أصحاب مواقع «صور الاعتقال» كميات ضخمة منها، وينشرونها فيصبح بإمكان أي شخص الوصول إليها. وبعدها، يطلبون مالاً ممن يرغب في إزالة صورته من تلك المواقع. إنّه ابتزاز، على الرغم من كونه قانونياً بالمعنى التقني. لن تختفي تلك الأشياء، على الرغم من أن القانون ربما حظر أحياناً بعضاً منها.

نحتاج إلى التفكير بتلك الأمور. يستطيع كل شخص أن يشتري إحدى الأدوات المتقدّمة في الرقابة، ما يعني أننا نحتاج إلى أعراف اجتماعيّة بصدد استعمالها أو عدمه. يعرف كل منّا عن الآخر بأكثر مما نرتاح له، لذا يجب تطوير أعراف اجتماعيّة بصدد الإقرار بما نعرفه أو التظاهر بأننا لا نعرف. سعى ديفيد برين أساساً إلى إثارة تلك النقطة الأساسيّة في كتابه **المجتمع الشفّاف** (Transparent Society)؛ بمعنى أن الرقابة الكليّة القدرة آتية، وعلينا التكيّف معها[28].

جسّدت الإنترنت الفجوة الأضخم بين الأجيال، منذ عهد موسيقى الـ «روك أند رول» في أوساط الخمسينيات من القرن العشرين. ووفق ما أشار إليه كلاي شيركي، لم يكن الأكبر سنّاً مخطئين بشأن التغييرات كافة التي توقّعوا أن تحدثها الـ «روك أند رول»، بل كانوا مخطئين بشأن مدى أذيتها[29]. يتأقلم البشر. عندما تخلّف الأفكار الشخصيّة لكل شخص منذ ولادته أثراً رقمياً عاماً، لن يفكر أي شخص مرّتين بشأن وجودها. إذا كانت التكنولوجيا تعني أن كل ما نقوله- كل تلك الاتهامات المؤسفة، والتفاهات كلها معاً- سيسجّل ويخزّن إلى الأبد، يغدو واجباً علينا أن نتعلّم كيف نعيش معها.

تكمن المشكلة في أننا بارعون جداً في التأقلم، على الأقل في المدى القريب. إذ إنّ الناس الذين يترعرعون في ظل وجود رقابة أكبر، يغدون أكثر ارتياحاً حيالها[30]. يرتاد بعضنا مدارس فيها آلات للتحقّق إلكترونيّاً من بطاقات الهويّة وأجهزة كشف المعادن[31]. يعمل بعضنا في مبانٍ تطلب تفحص الشارات الشخصيّة يوميّاً. ومن يسافرون جوّاً في الولايات المتّحدة، باتوا معتادين على إجراءات التفتيش من قِبَل «أمن إدارة النقل». ولم يعد المتسوّقون كافة يتفاجأون بأخبار السرقات الكبرى لبيانات بطاقات الائتمان. تلك هي الطُرُق التي روّضنا بها أنفسنا على القبول بخصوصيّة أقل. وعلى غرار كثير من الحقوق الأساسيّة، تمثّل الخصوصيّة أحد تلك الأشياء التي نلاحظها عندما نفقدها. إنّه لأمر مؤسف؛ لأنه بعد غيابها يصبح من الصعب استرجاعها.

يجب وقف الانحدار. أساساً، الجدال حول الخصوصيّة هو أخلاقي. إنّ الخصوصيّة شيء يجب أن نمتلكه، ليس لكونه مربحاً أو عملياً، بل لأنه أخلاقي. يجب إلقاء الرقابة العامة في مزبلة التاريخ، لتضاف إلى ممارسات كثيرة عدّها البشر ذات مرّة أمراً طبيعيّاً، لكننا ننظر إليها كونيّاً باعتبارها بغيضة. إنّ الخصوصيّة حق من حقوق الإنسان[32]. ليست تلك فكرة جديدة. إذ جرى الاعتراف بالخصوصيّة بوصفها حقاً أساسيّاً في «الإعلان العالمي لحقوق الإنسان» (1948)، و«الميثاق الأوروبي لحقوق الإنسان» (1970)[33].

توجد الخصوصيّة في دستور الولايات المتّحدة، ليس بصورة صريحة، لكنها متضمّنة في التعديلات 4 و5 و9 فيه[34]. ومثّلت الخصوصيّة جزءاً من «شرعة الحقوق الأساسيّة في الاتحاد الأوروبي» (2000)[35]. في 2013، أقرّت الجمعية العامة للأمم المتّحدة قراراً عنوانه «الحق في الخصوصيّة في العصر الرقمي»، الذي شدّد على تطبيق الحق الأساسي في الخصوصيّة على شبكة الإنترنت وخارجها، وأنّ خطر الرقابة العامة ينسف ذلك الحق[36].

"شرعة الحقوق الأساسيّة في الاتحاد الأوروبي" (2000)[37]

البند 7. احترام الحياة الشخصيّة والعائليّة. لكل شخص الحق في أن تحترم حياته/ حياتها الشخصيّة والعائليّة، وكذلك المنزل والاتّصالات.

البند 8. حماية البيانات الشخصيّة. 1 - لكلٍّ الحق في حماية البيانات الشخصيّة المتعلّقة به/ بها. 2 - يجب التعامل مع تلك البيانات بطريقة عادلة تخدم غايات محدّدة، استناداً إلى موافقة الشخص المعني بها، أو أُسس شرعيّة أخرى يقرّها القانون. 3 - يجب أن يوضع التحقّق من إطاعة تلك القواعد، بيد سلطة مستقلّة.

يُحتَفى بتلك المبادئ في القانون وطنيّاً ودوليّاً. يجب علينا الشروع في اتّباعها. ليست الخصوصيّة رفاهية يمكننا أن نحظى بها في أوقات الأمان وحدها. بالأحرى، إنّها قيمة يجب حمايتها. إنّها أمر أساسي للحريّة والاستقلاليّة والكرامة الإنسانيّة. يجب أن نفهم أن الخصوصيّة ليست أمراً قابلاً لأن نتخلّص منه في سياق محاولة مذعورة لضمان الأمن، بل إنّها شيء يجب صيانته وحمايته من أجل الحصول على أمن حقيقي[38].

لن يحصل شيء من ذلك من دون تغيير التوجّه. في خاتمة المطاف، سنحصل على الخصوصيّة التي نطالب بها نحن كمجتمع، وليس أكثر من ذلك بقلامة ظفر.

لا تنتظر. كلما أطلنا انتظار التغيير، صار أمره أشد صعوبة. من ناحية الشركات، باتت ممارسة الرقابة الشاملة والإعلانات المشخصنة عرفاً سارياً، وتحوز الشركات مجموعات ضغط سياسيّة تتكفل بتبديد محاولات التغيير.

يقدّم «قانون كاليفورنيا لعدم التتبع» مثلاً عن ذلك. إذ ابتدأ كفكرة حسنة، لكنه بات منزوع الأنياب كليّاً عند إقراره. يتكفلّ المسار الطبيعي لتقنية الرقابة (أتذكُر الحديث عن انخفاض تكلفة الرقابة في الفصل 2؟)، وإرساء أمر واقع جديد، بجعل النجاح في إحداث التغييرات أمراً أكثر صعوبة في المستقبل، خصوصاً في الولايات المتّحدة.

ليست الشركات وحدها من يقاوم التغيير. إذ يرغب السياسيّون في البيانات عينها التي يسعى إليها المعلِنون، وهي: البيانات الديموغرافيّة، والمعلومات عن التفضيلات الفرديّة للمستهلك، والمعتقدات الدينيّة والسياسيّة. إنّهم يستخدمونها في حملاتهم، ولن يتخلّوا عنها. من الصعب تماماً إقناعهم بالتخلي عن الوصول إلى معلومات تساعدهم في بثّ رسائل موجّهة، وحملات كشف التصويت وغيرها. وبمجرد أن يتوصّل أحدهم إلى فهم كيفيّة الاستفادة من تلك البيانات في جعل الانتخابات غير عادلة بصورة دائمة، على غرار ما يحصل عند التلاعب في التقسيم الإداري للمقاطعات لضمان ربح حزب معيّن؛ يغدو من الصعوبة بمكان إحداث التغيير.

في مؤتمر حضرته في 2014، تناهى إلى سمعي قول أحدهم: «إنّ «قسم التحليلات» في محرّك «غوغل» هو كوكايين من نوع الـ «كراك»، لرقابة الإنترنت. ما أن ترى تلك البيانات مرّة، حتى تصبح غير قادر عن التوقّف». بصورة أكثر عموميّة، تضحي البيانات هي مبرّر نفسها بحد ذاتها. كلما أطلنا الانتظار، تصبح أعداد متزايدة من الناس والمؤسّسات معتادة على الوصول الواسع لبياناتنا، ويتزايد أيضاً ميلها للقتال دفاعاً عن ذلك الوصول.

نحن في وقت ملائم على نحو فريد، كي نُحدِث تغييرات من الأنواع التي أوصيت بها في هذا الكتاب.

إن المؤسّسات التي تجمع بياناتنا وتتاجر بها قويّة، لكنها حديثة العهد نسبياً. كلما نضجّت وصارت أشد رسوخاً، سيغدو إحداث تغيير في طريقة عملها أشد صعوبة.

وضع سنودن الرقابة الحكوميّة تحت ضوء كاشف بإظهاره أفعال «وكالة الأمن القومي» و«قيادة الاتّصالات الحكوميّة». أدى ذلك إلى تنازع دولي فريد من نوعه، خصوصاً بين ألمانيا والولايات المتّحدة. واخترق ذلك التوتر السياسي الانقسام الحزبي في الولايات المتّحدة. يتيح ذلك الفرصة أمام تغيير حقيقي[39]. ووفق كلمات

رام إيمانويل عمدة شيكاغو والرئيس السابق لموظفي أوباما: «لا تفوّت فرصة حدوث أزمة فعليّة»[40]. ينطبق الأمر على هذا الوضع، على الرغم من أنّ معظم الناس لم يدرك أنها أزمة فعليّة.

نحن في لحظة فريدة في العلاقة بين الولايات المتّحدة والاتحاد الأوروبي. إذ يرغب الطرفان في تنسيق قوانينهما، وجعل التجارة بين حدودهما أكثر يسراً. من المحتمل أن تسير الأمور إلى أحد حدّين: إما أن تضحي أوروبا أشد تساهلاً كي تتناغم مع الولايات المتّحدة، أو أن تغدو الولايات المتّحدة أكثر صرامة كي تتناغم مع أوروبا. وعندما ستتساوى القوانين بين الطرفين، يصبح من الصعب تغييرها.

نعيش أيضاً لحظة فارقة في تاريخ العصر الرقمي. إذ أُدمِجَت الإنترنت في الأشياء كلّها. نستطيع رؤية تلك النُظُم مرحليّاً. بإمكاننا أن نُدخِل تغييرات عليها تستمر عقوداً.

حتى في تلك الحال، يجب أن نكون مستعدين لخوض ذلك كله كرّة أخرى.

إذ تتغيّر التكنولوجيا باستمرار، ما يجعل أشياء جديدة ممكنة، فيما تغدو القوانين السابقة متقادمة. لا سبب يدعونا للتفكير بأن تقنيّات الأمن والخصوصيّة وإغفال الهويّة، وهي التي تحمينا ضد مخاطر اليوم، ستكون مجدية غداً.

تتغيّر الحقائق السياسيّة أيضاً، وتتبدّل القوانين معها. من الغباء التفكير بأنّه إذا أرسينا مجموعة من الحلول اليوم، فلسوف تدوم إلى الأبد أو حتى إلى نصف قرن. يكفي إلقاء نظرة على التاريخ الأميركي الحديث لملاحظة أن الإساءات الكبرى لاستخدام السلطة التنفيذيّة– مع ما يرافقها من فضائح عامة كبرى وإصلاحات تخفيفيّة– تحدث كل 25 أو 30 سنة. من الأمثلة على ذلك «غارات بالمر»[*] في

(*) بين خريف 1919 وشتاء 1920، شنّت قوى الأمن بتفويض من المدعي العام ميتشيل بالمر، غارات على بيوت قادة النقابات العماليّة والاشتراكيين وبعض الفوضويّين، ورحلتهم قسراً عن الولايات المتّحدة. ولاحقاً، صارت الغارات من رموز الاعتداء على الحريّات والحقوق الأساسيّة للمواطن في أميركا.

عشرينيات القرن العشرين، والمكارثيّة في خمسينيات القرن نفسه، وإساءة استعمال سلطة الـ «إف بي آي» و«وكالة الأمن القومي» في سبعينيات ذلك القرن أيضاً، والإساءات الجارية لاستخدام السلطة عقب 9/ 11 في مطلع القرن الجاري.

إذا أمعنت التفكير في الأمر، تمثّل الثلاثون سنة متوسط مدّة عمل الموظّف المحترف في القطاع الحكومي. ويخامرني ظنّ بأن الأمر ليس مصادفة. ما يبدو أنه يجري هو أننا نحدث إصلاحات، ونتذكّر لفترة لماذا أدخلناها، وفي النهاية يتغيّر عدد كاف من الناس في الحكومة، فنبدأ بنسيان الأمر، ثم نعود كرّة ثانية إلى الإصلاحات ويجب علينا البدء بها مجدداً ضمن سياق تقني جديد.

سيتعين على جيل آخر أن ينهض بالمحاسبة على المجموعة التالية من إساءة استخدام السلطة. وستكون تلك اللحظة لنا.

ينتابني قلق من أننا لسنا جاهزين تماماً. إنّها مسألة تعاقب أجيال، ومنوط بالجيل التالي إحداث النقلات الاجتماعيّة اللازمة لتفعيل تغييرات سياسيّة تحمي خصوصيتنا الأساسيّة. أخشى أن الجيل الذي يتولّى الأمور حاضراً مصاب بذعر فائض من الإرهابيّين، ويتسرّع في إعطاء الشركات كل ما ترغب به. أرجو أن أكون مخطئاً.

مقايضة «البيانات الضخمة»

تناول معظم هذا الكتاب سوء استعمال بياناتنا الشخصيّة ورداءته. في المقابل، لا بد من الإقرار بأنّ البيانات تملك قيمة لا تصدّق في المجتمع.

تحوز بياناتنا قيمة كبرى عندما تُجمَع معاً. إذ تساعد سجلات تحرّكاتنا في تخطيط الإعمار الحضري. وتمكّن سجلاتنا الماليّة الشرطة من اكتشاف الفساد وتبييض الأموال ومنعها أيضاً. وتساعد تدويناتنا وتغريداتنا البحّاثة في فهم ما يتفاعل في

المجتمع. هنالك كل أنواع الاستعمالات الإبداعيّة والمؤثّرة لبياناتنا الشخصيّة، ويتولّد منها معارف جديدة تحسّن حياتنا.

وكذلك تملك بياناتنا قيمة لكل منا إفراديّاً، كي نُظهر منها أو نخفي ما نريد. وهنا تظهر العقدة. إذ يراهن استخدام البيانات على مصلحة المجموعة في مواجهة المصلحة الذاتيّة، وهو قلب تنازع ما فتأت الإنسانيّة تخوض فيه منذ وجودها الأول(41).

لنتذكّر الصفقات التي تحدّثت عنها في مقدّمة الكتاب. تمنحنا الحكومة صفقة: إذا أتحت لنا الحصول على بياناتك كلّها، يمكننا أن نحميك من الجريمة والإرهاب. إنّها صفقة مخادعة، بل عديمة الجدوى أيضاً. إنّها تضخيم أمن المجموعة على حساب أمن الفرد.

يمنحنا «غوغل» صفقة مماثلة، وهي غير متوازنة على نحو مماثل: إذا أتحت لنا الحصول على بياناتك كلّها وتخليت عن خصوصيّتك، سنعرض عليك الإعلانات التي ترغب في رؤيتها، ونمنحك مجانيّة البحث على الإنترنت، والبريد الإلكتروني وأنواع الخدمات الأخرى كلّها. لا تتمكّن شركات كـ«غوغل» و«فيسبوك» من عرض تلك الصفقات، إلا إذا تخلّى عدد كبير منّا عن الخصوصيّة. إذاً، لا تستطيع المجموعة الاستفادة إلا إذا رضخ عدد كبير من الأفراد.

لا تتسم بالقسوة كل تلك الصفقات التي تراهن على مصلحة المجموعة في مواجهة مصلحة الفرد. إذ يوشك المجتمع الطبي على عقد صفقة مماثلة معنا: دعنا نحصل على بياناتك الطبيّة كافة، ولسوف نستخدمها في إحداث ثورة في الرعاية الصحيّة ونحسّن حياة كل فرد. في تلك الحال، أعتقد أنهم أحسنوا الصياغة. لا أعتقد أن كل شخص يستطيع فهم مدى استفادة الإنسانيّة من وضع بياناتنا الصحيّة كافة في قاعدة بيانات واحدة، وتمكين البحّاثة من الوصول إليها(42). من المؤكّد أنّ تلك البيانات شخصيّة على نحو لا يصدّق، ومن المؤكّد أنها ستصل إلى أيادٍ

غـير تلك التـي قُصِدَ أن تكون بمتناولها، وتسـتعمل لغير الغايـة منها. لكن في تلك الحال تحديداً، يبدو جلياً بالنسبة لي ضرورة تقديم مصلحة المجتمع في استعمال تلك البيانات. هناك كثيرون لا يوافقون على ذلك.

ثمـة مثل آخـر على التوازن الصحيح بـين مصلحتي المجموعة والفـرد. إذ حلّل راينـول جونكو، وهو باحث في شـؤون الـ «سوشـال ميديا»، عادات الدراسـة بين طلبتـه[43]. هنـاك كثير مـن الكتب عـلى الإنترنت، وتجمـع مواقع الكتب الشـبكيّة كميّـات ضخمة مـن البيانات عن كيفيّـة تفاعل الطلبـة مع المواد الدراسـيّة، وعدد المـرات التي يفعلون بهـا ذلك. ودعم جونكو تلك المعلومات مـع بيانات تأتّت من رقابة النشـاطات الحاسـوبيّة الأخرى لطلبته. إنّه ضرب من البحث المتعدّي بطريقة لا تصـدّق، لكن مـدّته كانت محـدودة، وأمدّته بمعرفة جديدة عن طريقة دراسة الطالـب الجيّد والسيء، كما طوّر تدخّلات تهدف إلى تحسـين عادات الدراسـة عند الطلبة. هل فاقت مصلحة المجموعة نظيرتها في الخصوصيّة بالنسـبة لمن شـاركوا في تلك الدراسة؟

وافـق الطلبة على وضعهم تحت الرقابة، وحصل بحـث جونكو على موافقة هيئة الأخـلاق في الجامعـة؛ ولكن، مـاذا عن التجـارب التي تجريها الشركات؟ لسـنوات طويلـة، دأب موقـع «أوكـي كيوبيد» على إجراء تجـارب على مسـتخدميه، مظهراً أو حاجبـاً صورهم على نحو انتقائي، مشـدداً أو مخففاً من إجراءات التوافق مع شروط الموقع؛ وذلك ضمن سعيه لتفحص تأثير تلك المتغيّرات في سلوك قاصدي الموقع[44]. بإمكانك أن تحاجج بالقول إن تلك التجربة علمتنا الكثير، لكن من الصعوبة بمكان تبرير التلاعب بالناس بتلك الطريقة من دون معرفتهم ولا موافقتهم[45].

المـرّة تلو المـرّة، يظهر التنازع عينه: قيمة المجموعـة في مواجهة قيمة الفرد. هناك قيمـة لبياناتنا الجماعيّة في تقييـم كفاءة البرامج الاجتماعيّـة[46]. هنالك قيمة لبياناتنا الجماعيّة بالنسـبة لبحوث السـوق. وتملـك قيمة أيضاً في تحسـين خدمات الحكومة.

هناك قيمة لدراسة الميول الاجتماعيّة، وتوقّع الميول المستقبليّة. يجب علينا الموازنة بين تلك المنافع من جهة، والمخاطر الناجمة عن الرقابة التي تمكّن من الحصول على تلك البيانات.

يتمثّل السؤال الكبير في التالي: كيف يمكننا تصميم نُظُم تستطيع الاستفادة من بياناتنا الجماعيّة بصورة تفيد المجتمع ككل، مع حماية الناس إفرادياً في الوقت نفسه؟ وباقتباس صيغة من «نظرية الألعاب»(*)، كيف نصل إلى «نقطة توازن ناش» في جمع البيانات، بمعنى إقامة توازن يفضي إلى محصلة نهائيّة مناسبة للجميع، حتى عندما نكف عن تكييف الأمور لأحد المُكوّنات المفردة؟

ذلك هو الأمر. تلك هي القضية الرئيسة في عصر المعلومات. باستطاعتنا إيجاد حل لها، لكنها تتطلّب تفكيراً متأنياً بشأن القضايا المحدّدة، وتحليلاً أخلاقيّاً عن تأثير الحلول المختلفة في قيمنا الأساسيّة.

قابلت بعضاً من النشطاء المتصلّبين بشأن الخصوصيّة الذين على الرغم من ذلك يفكرون بأنها ستكون جريمة ألا تضع بياناتك الطبيّة في قاعدة بيانات تشمل المجتمع الواسع. قابلت أناساً لا يعارضون الرقابة الأشد حميميّة من الشركات، لكنهم يريدون ألا تلمس الحكومة تلك البيانات. قابلت أناساً لا يعارضون رقابة الحكومة، لكنهم يعترضون على أي شيء تحركه الرغبة في الربح. قابلت كثيرين من الناس ممن لا يعترضون على أيٍّ مما سبق ذكره.

كأفرادٍ وكمجتمع، نحاول دوماً إقامة توازن بين قيمنا المختلفة. لا نتوصل إلى صيغة مثالية أبداً. لكن المهم هو أننا ننخرط بإرادتنا في تلك العملية. في أحيان كثيرة، يأتي التوازن لنا من الحكومات والشركات، وبواسطة أجندتهم الخاصة.

أيّاً كانت سياساتنا، يجب أن نضع يدنا فيها[47]. لا نريد أن تقرر الـ «إف بي آي» و«وكالة الأمن القومي» سراً، مستويات الرقابة الحكوميّة المتاحة بداهة على هواتفنا؛

(*) انظر ملاحظة في الفصل 13.

بـل نريد مـن الكونغرس أن يقرّر أموراً كهذه وعبر نقاش عـام ومفتوح. لا نريد أن تقرّر حكومات الصين وروسـيا مسـتويات القدرة على الحجب في الإنترنت؛ بل أن يتقرر ذلك بواسـطة هيئة ذات معايير دولية. لا نريد أن يقرر موقع «فيسـبوك» مدى الخصوصيّـة التـي نتمتع بها مـع أصدقائنا، بل نريـد أن نقرّر ذلك بأنفسـنا. إنّ تلك القـرارات كلهـا تفوق في حجمهـا وأهميتها أي منظّمـة مفردة. لذا، يجـب أن تتقرّر بواسطة مؤسّسة كبرى تكون أكثر شمولاً وتمثيلاً. نريد أن يكون الناس قادرين على الخوض في نقاشـات علنيّة عن تلك الأمور، وأن نكون «نحن الشعب» قادرين على محاسبة صُنّاع القرار.

غالباً ما أستعيد عبارة للقس مارتن لوثر كينغ: «قوس التاريخ طويل، لكنه ينحي صوب العدالة»[48]. أنا متفائل على المدى الطويل، حتى لو بقيت متشائماً على المدى القصـير. أعتقد بأننا سـتتغلب على خوفنـا، ونتعلم كيف نعطي قيمـة لخصوصيّتنا، وأن نضـع القانـون في نصابه كي نحصد منافع «البيانات الضخمة»، مع الحفاظ على أمننا حيال بعض المخاطر. في اللحظة الراهنة، نحن نشهد بدايات حركة عالميّة قويّة لإقرار بالخصوصيّة كحق أسـاسي للإنسـان، وليـس بالمعنى المجرّد الـذي رأيناه في إعلانات عامة كثيرة؛ بل بطريقة متمكّنة ومحمّلة بالدلالات. يتولى الاتحاد الأوروبي القيادة، لكن آخرين يسـيرون معه. ستسـتغرق تلك العملية سنوات بل ربما عقوداً، لكنـي أعتقـد أنه بعد نصف قرن سـوف ينظر الناس إلى الممارسـات المعاصرة بشـأن البيانات بالطريقة نفسها التي ننظر بها نحن الآن إلى ممارسات مهنيّة سابقة بوصفها بدائيّـة ومهجـورة، كالزراعة المأجورة وعمالـة الأطفال ونقابات التجّـار في القرون الوسطى. تبدو تلك الأمور كلّها غير أخلاقيّة. إنّ نقطة البداية في تلك الحركة، أكثر من أي عنصر آخر، ستكون هي إرث إدوارد سنودن.

استـهللت الكتاب بالحديث عـن البيانات بوصفها «دخان العـادم»، بمعنى أنها شيء ما نتتجه جميعاً أثناء نشـاطاتنا في أعمال عصر المعلومات. وأعتقد أنني أسـتطيع السـير بذلك التشـبيه خطوة أبعـد. إذ عَدَّ البيانـات والمعلومات مشـكلة التلوّث في

عـصر المعلومات، وأنّ الخصوصيّة هي التحـدي البيئي. تنتج معظم الكومبيوترات معلومـات شـخصيّة؛ وهي تتلبـث، وتتعفّـن. وتكون كيفيّـة تعاملنـا معها- كيف نحتويهـا وكيـف نتخلّص منها- قضية أساسـيّة لصحة اقتصادنـا المعلوماتي. ومثلما ننظـر اليـوم إلى العقود الأولى من الثـورة الصناعيّـة، ونتعجّب من تجاهـل أجدادنا للتلوّث في خضم سـعيهم المحموم لبناء عالم صناعي؛ كذلك سينظر أطفالنا خلفهم لـيروا إلينا خلال العقـود الأولى لعصر المعلومات، ويحاكمونا على طريقة تعاملنا مع تحدي جمع البيانات وإساءة استعمالها.

فلنحاول أن نجعلهم فخورين.

تنويهات

بالنسبة لي، يشكل تأليف كتاب خوضاً في غمار الاستكشاف. لا أعرف أين سأصل، إلى أن أنتهي من الكتابة. يجعل ذلك من الصعب عليّ تسويق الكتاب. إذ لا أكتب عرضاً عاماً له. وأكاد لا أستطيع القول بدقّة ما الذي يتناوله الكتاب. ولا يستسيغ الناشرون تلك الأمور.

أولاً: يجب عليّ أن أشكر وكيلي في النشر إريك نلسون من وكالة «سوزان رابينر ليتيري إيجنسي»، الذي قدّم كتابي قبل أن يكون هناك كتاب. إذ اعتَقَد أنّه يستطيع تسويق «الكتاب التالي لشناير» للناشرين الرئيسيّين، بل إنّه اعتَقَد بتلك الفكرة إلى حدّ أنّه لم يطلب توقيع عقد قبل بدئه بالعمل.

ثانياً: يجب عليّ أن أشكر ناشر كتابي، جيف شريفيه، من «دار نورتون». إذ أبدى رغبته بشراء «الكتاب التالي لشناير» في ظل وجود توكيدات ضبابيّة عن موضوعه. كما أبدى قبوله بطريقتي في الكتابة.

لا أكتب الكتب من البداية إلى النهاية. بالأحرى أكتبها من تحت إلى فوق. أعني بذلك أنه في كل لحظات الكتابة، أكون منغمساً في العمل على الكتاب برمّته. يولّد ذلك أثرين غريبين: يتمثّل الأول في أنّ الكتاب يكون جاهزاً بمجرد شروعي في الكتابة. كل ما في الأمر أن الكتاب لا يكون في أفضل حال، لكنه يتحسّن مع استمراري في الكتابة. ويتمثّل الأثر الثاني في أنني أستمر في كتابة الكتاب وتحسينه إلى الأبد، لو أتيح لي ذلك. جلّ ما أفعله هو أنني أحدّد بطريقة اعتباطيّة النقطة التي أقول فيها «انتهى»، عندما يدنو زمن تسليم الكتاب.

تتيح لي تلك الطريقة الحصول على آراء تقييميّة أثناء عملية الكتابة. إذ قرأ كثيرون أجـزاء من مسـوّدة الكتاب أو طالعوها كلها، من بينهم: روس أندرسـون، سـتيف باس، كاسـبر بويدن، كودي شـاريت، ديفيد كامبل، كارين كوبـر، دوروثي دينيغ، كوري دوكتورو، ريان إليس، آديسـون فيشر، كاميل فرانسوا، ناعومي غيلنز، جون غيلمور، جاك غولد سـميث، بوب غورلاي، بيل هردل، ديبورا هورلاي، كريسـا جاكسون، راينول يونكو، جون كلزاي، ألكسندر كليمبورغ، ديفيد ليفاري، ستيفن ليبـه، هـاري لويس، يـون لي، كين ليو، آلكس لوميس، ساشـا ماينراث، اليشـيا إم. ماكدونالد، بابلو مولينا، رامز نعّام، بيتر نيومان، جوزيف ناي، كرستين باين، ديفيد م. بيري، ليبه بلونكت، ديفيد برينتس، باراثا راغافان، مارك روتنبرغ، مارتن شناير، سيث ديفيد شيون، آدم شوستاك، بيتر سواير، كيت والش، سارة م. واتسون، ديفيد واينبرغر، داسـتن وينزل، مارسي ويلر، ريتشارد ويللي، بن ويزنر، جوزفين وولف، جوناثان زيترain وشوشانا زوبوف. قدّم لي كل منهم اقتراحات أدمجتها في الكتاب.

كان لحفنة من الأشـخاص مسـاهمة لا تقدر بثمن في وضع هذا الكتاب. وكانت كاثلـين كايتـل أفضـل باحثـة عرفتهـا على الإطـلاق، وصرت غـير قادر عـلى تخيّل تأليف كتاب من دون مسـاعدتها. ينطبق الأمر عينه على ريبيكا كسـلر التي حرّرت الكتـاب مرّتـين أثناء عملية كتابتـه، وأعطتني اقتراحات نقديّة في كل مرّة. واسـتمر بيث فريدمان الذي تولى إعادة تحرير كل ما كتبته خلال السـنوات العشر الأخيرة في إثبات أنه شخص لا غنىً عنه.

أريـد أن أتوجّـه بالشـكر أيضاً لإدوارد سـنودن الذي أدت أفعاله الشـجاعة إلى إثـارة النقـاش العالمي الذي انخرطنا فيه عن الرقابة. ليـس مبالغة القول إنّني لم أكن لأكتب هذا المؤلَّف لو لم يفعل سـنودن ما فعله. وكذلك كان أمراً حسـناً قراءة تلك الوثائـق التي سرّبها، خصوصاً أنني كنـت مراقباً لأفعال «وكالة الأمن القومي» منذ سنوات طويلة.

ثمة ملاحظة بصـدد العنوان. لقد أحببتُ وناشري عنـوان المعلومات وجالوت بصـورة فوريّـة، لكن برزت مشـكلة أيضاً. إذ نـشر مالكوم غلادويل كتابـاً بعنوان ديفيـد وجالوت، قبل وقت قصير. لم يكن ذلك سـيّئاً تماماً، لكن كتابي السـابق حمل عنوان كَذَبَة ومتمردون، ونُشر مباشرة بعد صدور كتاب لغلادويل عنوانه منشقّون. وبـدا أمراً مفرطاً تقليدي لغلادويل مرّتين. في نيسـان (إبريل)، شرحتُ إشـكاليتي تلك على مُدوّنتي الإلكترونيّة. وفجأة، تلقيتُ رسالة إلكترونيّة من غلادويل تقول: «أحببـتُ المعلومـات وجالـوت..». لذا، اسـتندت إلى بركته ودعابتـه، وأبقيتُ على العنوان.

كتبـتُ هـذا المؤلَّف أثناء فترة الزمالـة في «معهد بركمان للإنترنـت والمجتمع» في «كليّة القانون» بـ «جامعة هارفرد»، ولا أسـتطيع أن أفي بالشـكر لكل الأشـخاص هنـاك. إذ سـاعدني الوقت الـذي قضيته مع زملائي وأسـاتذة «جامعـة هارفرد» في التفكـير بالقضايـا التي أثرتهـا في الكتاب؛ وكذلك الحال بالنسـبة للطلبة في مجموعة القـراءة التي توليت قيادتها في ربيع العـام 2014. ومنذ كانون ثاني (يناير) 2014، توليـت منصـب «المديـر الرئيـس للتكنولوجيـا» في شركـة «ريزيليانـت سيسـتمز» (Resilient Systems)، ويجب عليّ شـكرهـم أيضاً. وعلى رغم أن الكتاب لا يتصل مباشرة بما نقوم به في تلك الشركة، فإنهم أرخوا لي العنان كي أكتبه.

في الختـام، أود أن أشـكر أصدقائـي، وخصوصـاً زوجتـي كارين كوبـر، الذين تـآزروا معي للوصول إلى مزاج «تأليف كتـاب». أدرك جيّداً أن الكتاب الحالي أكثر سهولة من الذي سبقه، لكنه كان صعباً أيضاً.

أشكركم جميعاً.

عن المؤلّف

يحظى بروس شـنايـر بشـهرة دوليّـة عن كونـه اختصاصيّـاً تقنيّـاً في الأمن، بل أطلقـت عليه مجلة الإيكونومسـت لقـب «معلّم الأمن». وضع شـنايـر 12 كتاباً من بينها كَذَبَة ومتمردون: تفعيل الثقة التي يحتاجها المجتمع لينمو (2012)، إضافة إلى مئات المقالات والدراسـات والأوراق الأكاديميّة. ويتابع قرابة ربع مليون شخص نشرتـه الإخباريّة «كريبتو- غـرام» (*Crypto- Gram*) ومُدوّنته الإلكترونيّة «شـنايـر يتحـدث عن الأمـن» (*Schneier on Security*). ويتمتّع شـنايـر بدرجـة الزمالة من «مركز بركـمان للمجتمع والإنترنت» (*Berkman Center for Internet & Society*) التابـع لـ «كليّة هارفرد للحقوق»، والزمالـة في برنامج «المعهد المفتوح للتكنولوجيا في مؤسّسـة أمـيركا الجديـدة» (*New America Foundation's Open Technology Institute*)، وهو عضو مجلس إدارة في «مؤسّسـة الحدود الإلكترونيّة» (*Electronic Frontier Foundation*)، وعضـو المجلـس الاستشـاري في «مركـز معلومـات الخصوصيّـة الإلكترونيّـة» (*Electronic Privacy Information Center*). وكذلـك يعمل مديراً في مؤسّسة «ريزيليانت سيستمز».

يمكن قراءة مدوّنته الإلكترونيّة ومقالاته وأوراقه الأكاديميّة في موقع (*schneier.com*). ويمكن متابعة تغريداته في صفحته (*@schneierblog*).

كتب مختارة لبروس شناير

استمر: نصيحة صائبة من شناير حول الأمن (2013)

Carry On: Sound Advice from Schneier on Security (2013)

كَذَبَة ومتمردون: تفعيل الثقة التي يحتاجها المجتمع لينمو (2012)

Liars and Outliers: Enabling the Trust That Society Needs to Thrive (2012)

شناير يتحدث عن الأمن (2008)

Schneier on Security (2008)

ما وراء الخوف: التفكير بمنطقيّة حول الأمن في عالم غير مستقر (2003)

Beyond Fear: Thinking Sensibly about Security in an Uncertain World (2003)

أسرار وأكاذيب: الأمن الرقمي في عالم تربطه الشبكات (2000)

Secrets and Lies: Digital Security in a Networked World (2000)

التشـفير التطبيقـي: بروتوكـولات العمـل، والخوارزميّات، وشـيفرة المصدر في برنامج «سي» (1994 و1996)

Applied Cryptography: Protocols, Algorithms,and Source Code in C (1994 and 1996)

الهوامش

مدخل

1. ديفيد كراندال وآخرون (8 ديسمبر 2010)، مقال: «استنتاج الروابط الاجتماعيّة من المصادفات الجغرافيّة».
Proceedings of the National Academy of Sciences of the United States of America 107,
http://www.pnas.org/content/107/52/22436.short

2. برهن السياسي الألماني مالته سبيتز عن قوّة دمج بيانات المواقع الجغرافيّة بإعطائه معلومات عن أمكنة وجوده يومياً للصحافيّين. مقال في «زايت أون لاين» (مارس 2011): «التليفون يخبر كل شيء».
Zeit Online (Mar 2011), «Tell-all telephone,» *Zeit Online*,
http://www.zeit.de/datenschutz/malte-spitz-data-retention

3. مانليو دي دومينيكو وأنطونيو ليما وميركو ميزوليزي (في 18 و 19 حزيران/ يونيو2012)، مقال: «الاعتماد المتبادل وتوقعيّة التحرّك الإنساني والتفاعلات الاجتماعيّة».
Nokia Mobile Data Challenge Workshop, Newcastle, UK,
http://www.cs.bham.ac.uk/research/projects/nsl/mobility-prediction

4. التنسيق بين بيانات أبراج الخلوي وتسجيل المكالمات صوتيّاً على الأشرطة، يمثّل دليلاً قويّاً في المحاكم عن عدم مصداقية من يدافع عن نفسه؛ لأنها تبرهن كذبه بواسطة إظهار كلماته بالذات. شكّل ذلك دليلاً في إدانة سكوت بيترسون في جريمة قتل زوجته في 2002؛ بعد أن تعاونت عشيقته أمبر فراي مع الشرطة. وكالة «أسوشيتيد برس» في (27 آب/أغسطس 2004): «شهادة بيترسون تتحوّل إلى دليل إدانة في الحواسيب»، صحيفة **يو إس داي تو داي**
USA Today,
http://usatoday30.usatoday.com/news/nation/2004-08-27-peterson_x.htm

5. إيفان بيريس وسيوبهان غورمان (15 حزيران/يونيو 2013)، مقال في وول ستريت جورنال: «الهواتف تترك آثاراً دالّة».
Wall Street Journal,
http://online.wsj.com/news/articles/SB10001424127887324049504578545352803220058

تريفور هيوز (7 كانون أول/ديسمبر 2013) مقال في «كولورادون»: «بيانات الهاتف تساعد في حل جريمتي مقاطعة لارمير».
Coloradoan,
http://archive.coloradoan.com/article/20131207/NEWS01/312070068/Cellphone-data-aided-solving-two-Larimer-County-murders.

6. تغالي الشرطة في دقّة تلك المعلومات وتدين أبرياء بناءً على تلك البيانات. الإيكونومست (6 أيلول/سبتمبر 2014)، مقال: «البرجان».
Economist,

http://www.economist.com/news/united-states/21615622-junk-science-putting-innocent-people-jail-two-towers.

مايك ماسنيك (9 أيلول/سبتمبر 2014) في «تيك ديرت»، مقال: «تبيّن أن البيانات المكانيّة للخلوية لا تقترب من الحقيقة، لكن الجميع مغرم بها».

Tech Dirt,

https://www.techdirt.com/articles/20140908/04435128452/turns-out-cell-phone-location-data-is-not-even-close-to-accurate-everyone-falls-it.shtml.

7. هيثر موري (22 يناير 2014)، «زي ليد»، نيويورك تايمس، مقال: «رسائل نصيّة مشؤومة أرسلت إلى المحتجين في كييف، تبعث الرعب في الإنترنت».

The Lede, New York Times,

http://thelede.blogs.nytimes.com/2014/01/22/ominous-text-message-sentto-protesters-in-kiev-sends-chills-around-the-internet.

8. ميتشيل إيزيكوف (18 فبراير 2010)، مقال في نيوزويك: «الـ«إف بي آي» يتتبع خلويات المشتبه فيهم، بلا مذكرات قضائيّة».

Newsweek,

http://www.newsweek.com/fbi-tracks-suspects-cell-phones-without-warrant-75099

9. ستيف أولانسكي (17 يناير 2013)، مجلة فوربس، مقال: «هل يكون الإعلان الموجه وفق مكانياً هو مستقبل التسويق المتحرك والإعلان المتحرك»؟

Forbes,

http://www.forbes.com/sites/marketshare/2013/01/17/is-location-based-advertising-the-future-of-mobile-marketing-and-mobile-advertising.

جون ماكديرموت (20 فبراير 2014) في «ديجي داي»، مقال: «لماذا تلتهم الشركات الكبرى للإنترنت التطبيقات المستندة إلى تحديد المكان؟»

Digiday,

http://digiday.com/platforms/apple-google-microsoft-yahoo-are-betting-on-mobile

10. أنطون ترويانوفسكي (21 مايو 2013)، مقال في وول ستريت جورنال: «شركات الهاتف تبيع بيانات المستهلكين».

Wall Street Journal,

http://online.wsj.com/news/articles/SB10001424127887323463704578497153556847658

راشيل كينغ (13 يوليو 2013)، وول ستريت جورنال بلوغز، مقال: «الخطر يتهدّد زبائن شركة «إيه تي أند تي» للهاتف».

CIO Journal, Wall Street Journal Blogs,

http://blogs.wsj.com/cio/2013/07/13/aclu-att-customer-privacy-at-risk

11. هياواثا براي (8 يوليو 2013)، واشنطن غلوب، مقال: «التنقيب في معلومات الخلوي لرسم بروفايلات شخصيّة».

Boston Globe,

http://www.bostonglobe.com/business/2013/07/07/your-cellphone-yourself/eSvTK1UCqNOE7D4qbAcWPL/story.html.

12. كريغ تيمبرغ (24 أغسطس 2014)، واشنطن بوست، مقال: «للبيع: نُظُم تتّبع مستخدمي الخلوي أينما كانوا في الكرة الأرضيّة».

Washington Post,

http://www.washingtonpost.com/business/technology/for-sale-systemsthat-can-secretly-track-where-cellphone-users-go-around-the-globe/2014/08/24/f0700e8a-f003-11e3-bf76-447a5df6411f_story.html

13. «فِرينت» (2014)

Verint (2014), «About Verint,»
http://www.verint.com/about.

14. «منظمة الخصوصيّة العالميّة» (2012). «تبيع شركة «كوبهام» تقنيّات مراكز للمراقبة، ورصد الهاتف، والرقابة التقنيّة والتتبّع المكاني. لا يفرض قانون التوريد البريطاني قيوداً على تلك التقنيّات، لذا فمن الممكن بسهولة أن تصل إلى أيد غير مأمونة».

https://www.privacyinternational.org/sii/cobham.

15. ضمّت القائمة الكاملة في 2011؛ الجزائر، أستراليا، النمسا، بلجيكا، بروناي، جمهوريّة التشيك، جورجيا، غانا، إيرلندا، الكويت، ليبيا، النرويج، باكستان، السعودية، سنغافورة، جمهورية سلوفينيا، إسبانيا، السويد، تايوان، تركيا، المملكة المتحدة والولايات المتحدة.

Cobham (2011), «Tactical C4I systems: Eagle–Close Combat Radio (CCR),»
https://s3.amazonaws.com/s3.documentcloud.org/documents/409237/115-cobham-tactical-c4i.pdf

16. كريغ تيمبرغ (24 أغسطس 2014)، واشنطن بوست، مقال: «للبيع: نُظُم تتّبع مستخدمي الخلوي أينما كانوا في الكرة الأرضيّة».

Washington Post,
http://www.washingtonpost.com/business/technology/for-sale-systemsthat-can-secretly-track-where-cellphone-users-go-around-the-globe/2014/08/24/f0700e8a-f003-11e3-bf76-447a5df6411f_story.html

17. توبياس إنغل (9 يناير 2009)، «نادي فوضى الكومبيوتر»، مقال: «تحديد مواقع الخلويات باستخدام نظام الإشارة رقم 7».

Chaos Computer Club,
http://berlin.ccc.de/~tobias/25c3-locating-mobile-phones.pdf.

18. كيفن أوبراين (28 أكتوبر 2012)، واشنطن بوست، مقال: «المعلومات التي تجمعها التطبيقات تمثّل مساحة رماديّة قانونيّاً».

New York Times,
http://www.nytimes.com/2012/10/29/technology/mobile-apps-have-a-ravenous-ability-to-collect-personal-data.html

19. توجد مجموعة من التطبيقات المشابهة، ولكن يقدّم «هالو سباي» مثلاً فاضحاً. وعلى الرغم من أن بيان رفع المسؤوليّة على الموقع الشبكي للتطبيق يورد أنّه مصمّم من أجل «التجسّس الأخلاقي للآباء»، أو كي يستخدم في «هاتف نقّال تملكه أو تملك موافقة ملائمة لترصّده»، فإن النص نفسه يتفاخر بقدرته على العمل «في نسق شبحي»، كما يخصّص صفحة للخيانة الزوجيّة.

http://hellospy.com.

20. إنّ «سبايس جيني» (SpaceGenie) هو تطبيق رقمي تجسّسي آخر. في العام 2014، أدين مديره التنفيذي واعتُقِل بتهمة بيعه في الولايات المتحدة. كريغ تيمبرغ ومات زاباتوسلي (29 سبتمبر 2014)، واشنطن بوست، مقال: «صانع سبايس جيني، وهو تطبيق تجسّسي، يعتقل في فرجينيا».

Washington Post,
http://www.washingtonpost.com/business/technology/make-of-app-used-for-spying-indicted-in-virginia/2014/09/29/816b45b8-4805-11e4-a046-120a8a855cca_story.html

21. سبنسر آنغ ولورين ويبر (22 أكتوبر 2013)، وول ستريت جورنال، مقال: «ملاحظة إلى الموظّفين: الرئيس يتجسّس».

Wall Street Journal,
http://online.wsj.com/news/articles/SB10001424052702303672404579151440488919138

22. بارتون غيلمان وآشكان سلطاني (04 ديسمبر 2013)، واشنطن بوست، مقال: «وفق وثائق سنودن: «وكالة الأمن القومي» تتبّع مواقع الخلويات في العالم».
WashingtonPost,
http://www.washingtonpost.com/world/national-security/nsa-tracking-cellphone-locations-worldwide-snowden-documents-show/2013/12/04/5492873a-5cf2-11e3-bc56-c6ca94801fac_story.html
بارتون غيلمان وآشكان سلطاني (10 ديسمبر 2013)، واشنطن بوست، مقال: «وثائق جديدة تكشف كيف تستنتج «وكالة الأمن القومي» العلاقات بتحليل البيانات المكانيّة للخلوي».
Washington Post,
http://www.washingtonpost.com/blogs/theswitch/wp/2013/12/10/new-documents-show-how-the-nsa-infers-relationshipsbased-on-mobile-location-data
جيمس غلانز، وجيف لارسون وآندرو دبليو لهرن، (27 يناير 2014)، نيويورك تايمس، مقال: «وكالات الاستخبارات تسترق توجيه البيانات من تطبيق الخلوي».
New York Times,
http://www.nytimes.com/2014/01/28/world/spy-agencies-scour-phone-apps-forpersonal-data.html.

23. لا نعرف بصورة قاطعة إذا كانت تلك المعلومات صحيحة. دانا بريست (21 يوليو 2013)، واشنطن بوست، مقال: «تغذّى نمو «وكالة الأمن القومي» من الحاجة لاستهداف إرهابيّين».
Washington Post,
http://www.washingtonpost.com/world/national-security/nsagrowth-fueled-by-need-to-target-terrorists/2013/07/21/24c93cf4-f0b1-11e2-bed3-b9b6fe264871_story.html.
رايان غالاهار (22 يوليو 2013)، موقع «سلايت»، مقال: «تقارير عن قدرة «وكالة الأمن القومي» على تتبّع الخلويات حتى حين تكون مغلقة».
Slate,
http://www.slate.com/blogs/future_tense/2013/07/22/nsa_can_reportedly_track_cellphones_even_when_they_re_turned_off.html.

24. بمقدار ما أعرف، استخدم بيتر سواير ذلك المصطلح. بيتر سواير وكنيزا أحمد (28 نوفمبر 2011). «مركز الديمقراطية والتكنولوجيا». مقال: «العصر الذهبي للرقابة مقابل التعتيم الشامل».
Center for Democracy and Technology,
http://www.futureofprivacy.org/wp-content/uploads/Going-Dark-Versus-a-Golden-Age-for-Surveillance-Peter-Swire-and-Kenesa-A.pdf.

25. بولي سبرنغر (26 يناير 1999)، مجلة وايرد، مقال: «شركة «صن» تتحدث عن الخصوصيّة: انسَ الأمر».
Wired,
http://archive.wired.com/politics/law/new/1999/01/17538

26. رئيس أركان الجيش الأميركي (11 آب 2011)، بيان مشترك: «عمليات مشتركة».
Joint Publication 3-0,
http://fas.org/irp/doddir/dod/jp3_0.pdf.

27. إريك شميدت ويارد كوهن (2013)، كتاب العصر الرقمي الجديد: إعادة رسم مستقبل الشعب والأمم والأعمال.
The New Digital Age: Reshaping the Future of People, Nations and Business, Knopf,
http://www.newdigitalage.com.

28. لم يشِر أحد إلى الصفقة، ولكن يردّد الجميع أنّ الرقابة ضروريّة لحمايتنا. باتريسيا زنغرلي وتبسّم زكريا (18 يونيو 2013)، مقال: «رئيس «وكالة الأمن القومي»: المشرّعون يدافعون عن برامج الرقابة»، «رويترز».
Reuters,
http://www.reuters.com/article/2013/06/18/us-usa-security-idUSBRE95H15O20130618.
تلفزيون «الجزيرة» (29 أكتوبر 2013): «رئيس «وكالة الأمن القومي» يدافع عن برنامج التجسّس بمواجهة

احتجاج من الحلفاء».
Al Jazeera,
http://america.aljazeera.com/articles/2013/10/29/nsa-chief-defendsspyprogramamidusriftwitheurope.html.

29. أشار يفغيني موروزوف، وهو من نقّاد التكنولوجيا، تلك النقطة. يفغيني موروزوف، (22 أكتوبر 2013)، مجلة إم آي تي تكنولوجي ريفيو، مقال: «المشكلة الرقابة فعليّاً».
MIT Technology Review,
http://www.technologyreview.com/featuredstory/520426/the-real-privacy-problem

الفصل 1: المعلومات منتجاً جانبياً للحوسبة

1. بيتر إيكرسلي (يوليو 2010)، مقال: «ما مدى فرادة متصفّحك للإنترنت»؟
Proceedings of the 10th International Conference on Privacy Enhancing Technologies, Berlin, https://panopticlick.eff.org/browser-uniqueness.pdf.

2. بن فويدايلا (21 فبراير 2012). مقال: «كيف يعمل: الكومبيوتر في سيّارتك».
Popular Mechanics,
http://www.popularmechanics.com/cars/how-to/repair/how-it-works-the-computer-inside-your-car.

3. نايت كاردوزو (23 يوليو 2013). مقال في «مؤسّسة الحدود الإلكترونيّة» بعنوان: «فرض صناديق سود في السيّارات هو تعدٍّ على الخصوصيّة».
Electronic Frontier Foundation,
https://www.eff.org/press/releases/mandatory-black-boxes-cars-raise-privacy-questions.

4. لوكاس مياريان (23 يوليو 2013). مقال في مجلة عالم الكومبيوتر بعنوان: «السيارة الذاتيّة القيادة تولّد 01 غيغابايت من البيانات في الثانية».
Computer World,
http://www.computerworld.com/s/article/9240992/Self_driving_cars_could_create_1GB_of_data_a_second.

5. بنجامين هين، ماكسمليان كوخ وماثيو سميث. (-3 7 مارس 2014)، ورقة بحثيّة بعنوان: «عن التوعية والسيطرة والخصوصيّة، بشأن «البيانات الوصفيّة» التي تحتويها الصور المتشاركة».
Distributed Computing & Security Group, Leibniz University, presented at the Eighteenth International Conference for Financial Cryptography and Data Security, Barbados,
http://ifca.ai/fc14/papers/fc14_submission_117.pdf.

6. الحال أن تلك القصة بالتحديد هي مريبة تماماً، بشأن الـ«ميتاداتا» في الكاميرا. ماثيو هونان (19 يناير 2009)، مجلة وايرد، مقال بعنوان: «أنا هنا: قصة عن تجربة عيش رجل يعي أهمية بيانات المواقع».
Wired,
http://www.wired.com/gadgets/wireless/magazine/17-02/lp_guineapig.

7. باطّراد، تعمل الحكومات على إزالة خيار الدفع نقداً المغْفَل الهويّة. آدريان جفريس (27 مارس 2013)، مقال: «نظام الدفع غير النقدي عند «جسر البوابة الذهبيّة» يعد بالراحة مقابل الخصوصيّة».
Verge,
http://www.theverge.com/2013/3/27/4150702/golden-gate-bridges-new-cashless-tollway-promises-convenience-for-privacy.

آناه دو (20 مارس 2014)، صحيفة لوس أنجلوس تايمس، مقال: «العبور في شوارع مقاطعة «أورانج»

بآليّة الدفع غير النقدي».
Los Angeles Times,
http://www.latimes.com/local/lanow/la-me-ln-cashless-toll-roads-20140320-story.html

تريفور بيتيفور (13 يونيو 2014)، مقال: «نظام عبور الشوارع في «فتيران» تصبح آلية الدفع».
Bay News 9,
http://www.baynews9.com/content/news/baynews9/news/article.html/content/news/articles/bn9/2014/6/13/veterans_expressway_.html.

مارتين باورز (17 يوليو 2014)، بوسـطن غلوب، مقال: «بداية من الاثنين، لا دفع نقديٌّ في بوابات شـوارع «توبين»».
Boston Globe,
http://www.bostonglobe.com/metro/2014/07/16/starting-monday-more-cash-tobin/WZKMDilsfLULQtYiGZCrEK/story.html.

8. «نِست» (2014). «آلة تنظيم حرارة «نِست» قادرة على التعلّم».
http://certified.nest.com/resources/NEST_POS_brochure_r7_300.pdf

9. إليزا باركلي (4 مايو 2012)، مقال: «الثلاجة الذكيّة تكتشف الخسّة المفقودة، مقابل ثمن».
The Salt: What's On Your Plate, NPR,
http://www.npr.org/blogs/thesalt/ 2012/05/03/ 151968878/the-smart-fridge-finds-the-lost-lettuce-for-a-price.

10. راي كريست (8 يونيو 2014). مقال: «مكيف الهواء الذكي من «هايير» أولًا في كونه مجازاً من «آبل» بين أنواع التجهيزات المنزليّة».
CNET,
http://ces.cnet.com/8301-35306_1-57616915/haiers-new-air-conditioner-is-the-first-apple-certified-home-appliance

11. هيثر كيلي (15 يناير 2014). مقال: «يرغب «غوغل» في السيطرة على منزلك بواسطة شركة «نِست»». شبكة «سي آن آن».
CNN,
http://www.cnn.com/2014/01/15/tech/innovation/google-connect-home-nest.

12. «وزارة الطاقة الأميركيّة». دراسة: «مدخل إلى شبكات الكهرباء الذكيّة». (2008).
http://energy.gov/sites/prod/files/oeprod/DocumentsandMedia/DOE_SG_Book_Single_Pages(1).pdf.
US Department of Energy (2014), «What is the smart grid?» https://www.smartgrid.gov/the_smart_grid.

13. غريغوري فرينشتاين. مقال: «كيف تستطيع آلات تتبّع المؤشّرات الصحيّة خفض الخيانة الزوجيّة».
Tech Crunch,
http://techcrunch.com/2013/07/05/how-health-trackers-could-reduce-sexual-infidelity

14. قاعدة بيانات «فِت بِت» (3 ديسمبر 2013).
Privacy policy,
http://www.fitabase.com/Privacy.

15. سارة إي. نيدلمان (14 أغسطس 2012). وول ستريت جورنال. مقال: «أدوات طبيّة جديدة وذكيّة».
Wall Street Journal,
http://online.wsj.com/news/articles/SB10000872396390444318104577587141033340190

16. ســارة واطســون (10 أكتوبر 2013). مجلة وايرد. مقال: «الهواتف الذكيّة الأكثر حداثة تســتطيع أن تحوّلنا جميعاً أدوات لتتبّع النشاطات».
Wired,

http://www.wired.com/2013/10/the-trojan-horse-of-the-latest-iphone-with-the-m7-coprocessor-weall-become-qs-activity-trackers.

17. توماس غويتز (17 نوفمبر 2007). مجلة وايرد مقال: «شركة «23أند مي» ستفكك شيفرتك الوراثية لقاء 1000 دولار. أهلاً بكم في عصر المعلوماتيّة الجينيّة».

Wired,

http://www.wired.com/medtech/genetics/magazine/15-12/ff_genomics.

إليزابيث موري (14 أكتوبر 2013). مقال: «جولة في أفكار مؤسّسة «23أند مي» آنا فويسيكي عن ثورة الـ99 دولارا».

Fast Company,

http://www.fastcompany.com/3018598/for-99-this-ceo-can-tell-you-whatmight-kill-you-inside-23andme-founder-anne-wojcickis-dna-r.

18. تشارلز زايفه (27 نوفمبر 2013). مجلة **ساينتيفك أميركان**. مقال: «شركة «23أند مي» مخيفة لأسباب غير التي يفكر فيها «مكتب الغذاء والدواء»».

Scientific American,

http://www.scientificamerican.com/article/23andme-is-terrifying-but-not-for-reasons-fda

19. ريبيكا غرينفيلد (25 نوفمبر 2013). مقال: «لماذا تخيف شركة «23أند مي» شركات التأمين الصحي».

Fast Company,

http://www.fastcompany.com/3022224/innovation-agents/why-23andme-terrifies-health-insurance-companies.

20. ليو كيليون (6 يناير 2014). «بي بي سي»، مقال: «2014 «سي إي أس»: شركة «سوني» تتباهى بتطبيق يشكّل سجلاً للحياة».

BBC News,

http://www.bbc.com/news/technology-25633647

21. أليك ويلكنسون (28 مايو 2007). صحيفة **نيويوركر**. مقال: «أتذكّر ذلك؟ مشروع لتسجيل كل ما نفعله في الحياة».

New Yorker,

http://www.newyorker.com/reporting/2007/05/28/070528fa_fact_wilkinson

22. جينا وورثام (8 مارس 2013). **نيويورك تايمس بلوغز**. مقال: «تعرّف إلى «ميموتو» الكاميرا التي تسجّل حياتك كلها».

New York Times Blogs,

http://bits.blogs.nytimes.com/2013/03/08/meet-memoto-the-lifelogging-camera

23. كين هيس (10 يناير 2014). مجلة **زد دي نِت**. مقال: «نظرة إلى إنترنت الأشياء في 2014: كل الأشياء متّصلة بالإنترنت وتتواصل مع بعضها بعضاً».

ZDNet,

http://www.zdnet.com/the-internet-of-things-outlook-for-2014-everything-connected-and-communicating-7000024930.

24. جورجينا ستايلويانو. (29 إبريل 2013). مقال: «الفكرة هي نشر مجسّات لتراقب كل شيء في المدينة».

Press (Christchurch),

http://www.stuff.co.nz/the-press/business/the-rebuild/8606956/Idea-to-have-sensors-track-everything-in-city.

فكتوريا تورك (يوليو 2013). مجلة وايرد. مقال: «مجسّات المدن: إنترنت الأشياء تستولي على مدننا».

Wired,

http://www.wired.co.uk/magazine/archive/2013/07/everything-is-connected/city-sensors

25. سام بايفورد (5 يناير 2014). مقال: «فراشي أسنان ذكيّة من شركة «كوليبري» تزعم أنها تحسّن صحة الأسنان ونظافتها».

Verge,
http://www.theverge.com/2014/1/5/5277426/kolibree-smart-toothbrush

26. مارغريت رودس (23 سبتمبر 2014). مجلة وايرد. مقال: «مهندسون من الـ«ناسا» وشركة «تسلا» يصنعون مصباح إنارة أكثر ذكاءً منك».
Wired,
http://www.wired.com/2014/09/ex-tesla-nasa-engineers-make-light-bulb-thats-smarter

27. ناقش تشارلز ستروس إملاءات تلك الأشياء. تشارلز ستروس (25 يونيو 2014). خطاب افتتاحي في جمعية مختصّة في نيويورك عن «البرمجة في 2034».
Charlie's Diary,
http://www.antipope.org/charlie/blog-static/2014/06/yapcna-2014-keynote-programmin.html

28. فالنتينا بالادينو (8 يناير 2014). مقال: «زجاجة دواء ذكيّة من شركة «آدهير تيك» تعرف متى أخذت دواءك، ومتى لم تفعل».
Verge,
http://www.theverge.com/2014/1/8/5289022/adheretech-smart-pill-bottle

29. موقع «إيكونوكوم» (19 سبتمبر 2013). مقال: «عندما تتلاقى الموضة مع إنترنت الأشياء».
emedia,
http://blog.econocom.com/en/blog/when-fashion-meets-the-internet-of-things.

30. لقد رأينا ذلك من قبل. إذ راجت الساعات الرقميّة في سبعينيات القرن العشرين. في البداية، كانت تلك أدوات مستقلة بحد ذاتها- تضم منبّهات وساعات-، ثم انخفض ثمنها. وصارت منبثّة في أشياء أخرى كفرن الـ«مايكروويف»، وسخّان القهوة، والفرن المنزلي، ومنظّم الحرارة، وجهاز الفيديو والتلفزيون. وتسير المجسّات المتّصلة بالإنترنت في الاتجاه عينه.

31. ناتاشا لوماس (9 مايو 2013). مقال: «مجسات «10 بي إن+» متّصلة لا سلكيّاً بالأشياء حاضراً، ومجسّات «30 بي إن+» ستكون متّصلة بإنترنت الأشياء في عشرينيات القرن الجاري؛ وفق بحث لمؤسّسة «إيه بي آي»».
Tech Crunch,
http://techcrunch.com/2013/05/09/internet-of-everything

32. فالنتينا بالادينو (10 يناير 2014). مقال: «الذكاء الخفي: كيف تستطيع المجسّات الدقيقة ربط كل الأشياء التي نملكها».
Verge,
http://www.theverge.com/2014/1/10/5293778/invisible-intelligence-tiny-sensors-that-connect-everything

33. بن هامرسلي (يوليو 2013). مجلة وايرد. مقال: «عندما يصبح العالم هو الـ«ويب»».
http://www.wired.co.uk/magazine/archive/2013/07/everything-is-connected/when-the-world-becomes-the-web

34. وضع مطار «نيوورك» تلك الإشارات. ديان كاردويل (17 فبراير 2014). صحيفة نيويورك تايمس. مقال: «إشارات السير في مطار «نيوورك» تعمل. إنّها تراقبك».
New York Times,
http://www.nytimes.com/2014/02/18/business/at-newarkairport-the-lights-are-on-and-theyre-watching-you.html

35. أولغا كاريف (31 أكتوبر 2013). صحيفة واشنطن بوست. مقال: «مع انتقال الـ«درون» من القطاع العسكري إلى المدني، المستثمرون يتدخّلون».
Washington Post,
http://www.washingtonpost.com/business/as-drones-evolve-from-military-to-civilian-usesventure-capitalists-move-in/2013/10/31/592ca862-419e-11e3-8b74-d89d714ca4dd_story.html.

36. بول ماكليري (29 يونيو 2014). مقال: «رادار قوي في منطاد، يراقب واشنطن (بلتيمور) وصولاً إلى البحر».
Defense News, http://www.defensenews.com/article/20140629/DEFREG02/306290012/Powerful-Radar-Blimp-Surveil-Washington-Baltimore-Out-Sea.

37. هناك الكثير من النقاش عن ذلك. «مؤسّسة الحدود الإلكترونيّة» (2014). مقال: «تلاعب الحكومة بالكلمات عند الحديث عن «وكالة الأمن القومي» والتجسّس الداخلي».
https://www.eff.org/nsa-spying/wordgames

38. يستند ذلك إلى تقدير منطقي بأن الصفحة المكتوبة تحتوي 2 كيلوبايت. وعلى الرغم من ذلك، لا يكون التقدير كاملاً؛ لأن معظم ذلك المحتوى هو ملفات للصوت والصورة وأشرطة الفيديو.

39. إم. جي. سيغلر (4 أغسطس 2010). مقال: «إريك شميدت: في كل يوم، ننتج من المعلومات بمثل ما فعلنا منذ 2003».
Tech Crunch,
http://techcrunch.com/2010/08/04/schmidt-data

40. شركة «سيسكو» (10 يونيو 2014). «مؤشّر «سيسكو» عن التشبيك البصري: المنهجيّة والتوقّعات، 2013 - 2018».
http://www.cisco.com/c/en/us/solutions/collateral/service-provider/ip-ngn-ip-next-generation-network/white_paper_c11-481360.html.

41. كريس إيفانز (18 إبريل 2014). مقال: «سلسلة الـ«آي إيه إيه أس»: تسعير التخزين في السحب الرقميّة: ما هو أدنى سعر ممكن؟».
Architecting IT,
http://blog.architecting.it/2014/04/18/iaas-series-cloud-storage-pricing-how-low-can-they-go

42. ك. يونغ (6 سبتمبر 2012). مقال: «ما هي تكلفة تخزين كل التغريدات العابرة في الخطوط؟».
Mortar: Data Science at Scale,
http://blog.mortardata.com/post/31027073689/how-much-would-it-cost-to-store-the-entire-twitter.

43. بروستر كاهيل (2013)، «تكلفة تخزين المكالمات الصوتية كافة لهواتف الولايات المتحدة في السنة، ما يتيح التنقيب على البيانات فيها».
https://docs.google.com/spreadsheet/ccc?key=0AuqlWHQKlooOdGJrSzhBVnh0WGlzWHpCZFNVcURkX0E#gid=0.

في العام 2013، أنهت «وكالة الأمن القومي». جيمس بمفورد (15 مارس 2012). مجلة وايرد. مقال: «شيّدت «وكالة الأمن القومي» أضخم مركز تجسّس (راقب كلامك)».
Wired,
http://www.wired.com/threatlevel/2012/03/ff_nsadatacenter/all

44. مجلة فوربس (19 أكتوبر 2012). مقال: «مراكز المعلومات الخمسة الأضخم في العالم».
Forbes,
http://www.forbes.com/pictures/fhgl45ijg/range-international-information-hub

45. كشمير هيل (24 يوليو 2013). مجلة فوربس. مقال: «مؤشّرات موثوقة عن «مركز يوتاه للمعلومات» الذي بنته «وكالة الأمن القومي» ببذخ سخيف، تدل إلى أنّه أقل قدرة على تخزين البيانات».
Forbes,
http://www.forbes.com/sites/kashmirhill/2013/07/24/blueprints-of-nsa-data-center-in-utah-suggest-its-storage-capacity-is-less-impressive-than-thought.

46. سيوبهان غورمان (21 أكتوبر 2013). صحيفة وول ستريت جورنال. مقال: «المقاولون يتقاتلون حول التأخّر في إنجاز مركز بيانات لـ«وكالة الأمن القومي»».
Wall Street Journal,
http://online.wsj.com/news/articles/SB10001424052702303672404579149902978119902

47. راندال مونرو (2013). «مراكز البيانات في «غوغل» تعمل بالبطاقات المثقّبة».
What If? XKCD,
https://what-if.xkcd.com/63

48. سـايروس فاريفـار (15 نوفمـبر 2012). مقـال: «كيـف أرغم طالـب قانون «فيسـبوك» على الحذر بشـأن الخصوصيّة».
Ars Technica,
http://arstechnica.com/tech-policy/2012/11/how-one-law-student-is-making-facebook-get-seriousabout-privacy.

أوليفيا سـولون (28 ديسـمبر 2012). هيئة الـدبي بي سي». مقال: «كم يملك «فيسـبوك» من المعلومات عن شخص واحد؟ 1200 صفحة من البيانات المتوزّعة على 57 صنفاً».
BBC News,
http://www.wired.co.uk/magazine/archive/2012/12/start/privacy-versus-facebook

49. ما اكتشفه شريمز حفزه على رفع دعوى من الدرجة الأولى ضد «فيسبوك». ليات كلارك (01 أغسطس 2014). مجلة وايرد. مقال: «إصابة «فيسبوك» بدعوى قضائيّة عالميّة».
Wired UK,
http://www.wired.co.uk/news/archive/2014-08/01/facebook-class-action-lawsuit

الفصل 2 : المعلومات بوصفها رقابة

1. ضمّت صفوف من سّربوا قبل سـنودن وثائق عن الوكالة، توماس دريك، مارك كلاين وبيل بيني. لحد الآن، لم يجر التعرّف إلى مسّربين بعد سنودن. بروس شناير (7 أغسطس 2014): «مجتمع الاستخبارات الأميركي فيه مُسّرب ثالث». كتاب شناير عن الأمن.
Schneier on Security,
https://www.schneier.com/blog/archives/2014/08/the_us_intellig.html

2. غلـين غرينوالـد (5 يونيو 2013). صحيفة الغارديان. «تجمع «وكالة الأمن القومي» سـجلات هواتف الملايين من زبائن شركة «فريزون» يوميّاً».
Guardian,
http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order

3. باراك أوباما (7 يونيو 2013). «تصريح رئاسي».
«Statement by the President,» US Executive Office of the President,
http://www.whitehouse.gov/the-press-office/2013/06/07/statement-president

جيمس كلايبر (7 يونيو 2013) «بيان من «الاسـتخبارات الوطنيّة» عن الكشف غير المصرّح به لوثائق سريّة»، مكتب رئيس «الاستخبارات الوطنيّة».
http://www.dni.gov/index.php/newsroom/press-releases/191-press-releases-2013/868-dni-statement-on-recent-unauthorized-disclosures-of-classified-information.

إد أوكيـف (6 يونيـو 2013)، صحيفة واشـنطن بوسـت، مقال: «مقتطـف: ديانا فاينشـتاين، وفق شرح ساكسباي شامبلس، تدافع عن برنامج «وكالة الأمن القومي» في التجسّس على الهواتف».
Washington Post,
http:// www.washingtonpost.com/blogs/post-politics/wp/2013/06/06/transcript-diannefeinstein-saxby-chambliss-explain-defend-nsa-phone-records-program

4. هل أنا وحدي من يشـتبه في سبب اسـتعمال الرئيس أوباما كلمات محدّدة بعينها؟ إذ يقول دائماً أشياء كـ«إنّ أحـداً لا يصغي إلى مكالماتك الهاتفيّة». ويترك ذلـك المجال مفتوحاً أمام إمكان أن تكون «وكالة الأمن القومي»،

تعمل على تسجيل وتوثيق وتحليل مكالمتك- وربما أحياناً تستمع إليها. الأرجح أن ذلك صحيح، وهو شيء يتيح لرئيس بعقلية ضيّقة أن يدّعي لاحقاً بأنّه لم يكن يكذب.

5. ثمة مقال جيّد عن مدى حميميّة الـ«ميتاداتا». داليا ليثويك وستيف فلاديك (22 نوفمبر 2013)، مقال: «حذف ما لا أهمية له من «البيانات الوصفيّة»».

Slate,

http://www.slate.com/articles/news_and_politics/jurisprudence/2013/11/nsa_and_metadata_how_the_government_can_spy_on_your_health_political_beliefs.html

6. إدوارد دبليو فلتين (23 أغسطس 2013). «إعلان من البروفسور إدوارد دبليو فلتين».

American Civil Liberties Union et al. v. James R. Clapper et al., United States District Court, Southern District of New York (Case 1:13-cv-03994-WHP), https:// www.aclu.org/files/pdfs/natsec/clapper/2013.08.26%20ACLU%20PI%20Brief%20-%20Declaration%20-%20Felten.pdf

7. إيف- ألكسندر دي مونتجوي وآخرون (2-5 إبريل 2013). ورقة بحث عن «توقّع شخصيّة الناس باستعمال طرق حسابيّة جديدة لتحليل بيانات الهواتف». قدّمت في «المؤتمر السادس عن الحوسبة الاجتماعيّة، النمذجة السلوكيّة- الثقافيّة والتوقع». واشنطن.

6th International Conferenceon Social Computing, Behavioral-Cultural Modeling and Prediction, Washington, D.C., http://realitycommons.media.mit.edu/download.php?file=deMontjoye2013predicting-citation.pdf.

8. تقدّم شركة «آي بي أم» مستوى مرتفعاً في تحليل الـ«ميتاداتا» للهواتف. شركة «آي بي أم» (2014). «9 تي 225 ج: تحليل معلومات الهاتف باستخدام دليل «آي2» للتحليل».

http://www.03.ibm.com/services/learning/content/ites.wss/zz/en?pageType=course_description&courseCode=9T225G&cc=.

9. جوناثان ماير وباتريك موتشلر (14 مارس 2014). مقال: «ميتافون: الطابع الحسّاس لمعلومات الـ«ميتاداتا».

Web Policy,

http://webpolicy.org/2014/03/12/metaphone-the-sensitivity-of-telephone-metadata

10. على الرغم من وضوح أنها بيانات وليس «بيانات وصفيّة»، يبدو أن «وكالة الأمن القومي» تعاملها كـ«بيانات وصفيّة». وأعتقد أن التبرير لذلك هو أن مفردات التفتيش تكون مشفّرة في العنوان الإلكتروني للموقع. إذ إن الشرائح الضوئيّة لـ«وكالة الأمن القومي» تتحدّث عن تجميع «عمليات التفتيش المستندة إلى الإنترنت»، ما يضيف وزناً إلى الاعتقاد بأن الوكالة تعاملها على أنها «ميتاداتا» وليس معلومات. غلين غرينوالد (13 يوليو2013). صحيفة الغارديان. مقال: «إكس كي سكور: وكالة الأمن القومي ترصد معظم ما يفعله مستخدم الإنترنت».

Guardian,

http://www.theguardian.com/world/2013/jul/31/nsa-top-secret-program-online-data

11. يثبت ذلك مجدّداً أن الفارق قانونيّاً هو أقل من شعرة.

12. تكرّر ذلك أيضاً مع عبارة: «هل يجب أن أخبر صديقتي»؟

13. أروى مهداوي (22 أكتوبر 2013). صحيفة الغارديان. مقال: «يكشف «غوغل» أفكارنا الأشد سوءاً».

http://www.theguardian.com/commentisfree/2013/oct/22/google-autocomplete-un-women-ad-discrimination-algorithms

14. دريـك طومســون (1 نوفمــبر 2010). مجلة آتلانتيـك. مقال: «المديـر التنفيذي لـ«غوغـل»: القوانين تكتبها مجموعات الضغط».
Atlantic,
http://www.theatlantic.com/technology/archive/2010/10/googles-ceo-the-laws-are-written-by-lobbyists/63908.

15. بإمكانـك التفتيـش عن معلومات عن نمط النوم لدى أيّ مسـتخدم لـ«تويتر». آميت أغـراوال (2013) «وقت النوم».
«Sleeping Time,» *Digital Inspiration*,
http://sleepingtime.org.

16. هناك دراستان عن الرسوم البيانيّة للعلاقات الاجتماعيّة على «فيسبوك»، تظهر مدى سهولة كشف تلك الأمور.
كارتر يارنغام وبهرام ر. ت. ميســتري (5 أكتوبر 2009). دراسـة: «اكتشـاف المثليّين بالحدس: «فيسـبوك» يكشف توجّهاتك الجنسيّة».
First Monday 14, http://firstmonday.org/article/view/2611/2302
مايكل كوزنســكي، ديفيد ســتلويل، وثور غرايبل (11 مارس 2013). دراسـة: «الميول الشخصيّة والانتماءات قابلة للتوقّع من السجلّات الرقميّة عن السلوك الإنساني».
Proceedings of the National Academy of Sciences of the United States of America (Early Edition),
http://www.pnas.org/content/early/2013/03/06/1218772110.abstract.

17. تسـتطيع أداة انغماسـيّة صنعها «مختـبر الميديا» في «معهد ماساشوسـتس للتقنية»، أن تصنع رسـماً بيانياً اجتماعياً عنك، استناداً إلى الـ«ميتاداتا» في بريدك الإلكتروني. «مختبر الميديا» (2013)، «انغماس: وجهة نظر مرتكزة إلى الناس في تحليل بريدك الإلكتروني».
https://immersion.media.mit.edu.

18. برايان لام (19 يونيو 2013). مجلة وايرد، مقال: «أوه... «وكالة الأمن القومي» لا تجمع سـوى الـ«ميتاداتا»، لكن يجب أن تبقى قلِقاً».
Wired,
http://www.wired.com/2013/06/phew-it-was-just-metadata-not-think-again.

19. إدوارد دبليو فلتين (23 أغسطس 2013). «تصريح من البروفسور إدوارد دبليو فلتين».
American Civil Liberties Union et al. v. James R. Clapper et al., United States District Court, Southern District of New York (Case 1:13-cv-03994- WHP),
https://www.aclu.org/files/pdfs/natsec/clapper/2013.08.26%20ACLU%20PI%20Brief%20-%20Declaration%20-%20Felten.pdf.

20. آلـن روس بريدجـر (21 نوفمبر 2013). نيويـورك ريفيو أوف بوكس. مقال: «كشـوفات سـنودن وعامة الناس».
New York Review of Books,
http://www.nybooks.com/articles/archives/2013/nov/21/snowden-leaks-and-public

21. ديفيد كول (10 مايو 2014). مقال: «نقتل الناس استناداً إلى معطيات الـ«ميتاداتا»».
New York Review of Books,
http://www.nybooks.com/blogs/nyrblog/2014/may/10/we-kill-people-based-metadata.

22. جيم أو. كوهلر. (1999). ستازي: القصة غير المعلنة للبوليس السري في ألمانيا الشرقيّة.
Westview Press,
http://books.google.com/books?id=waxWwxY1tt8C.

23. ماري دي روزا (2005). «البند 206: التوسّع في التنصّت تحت مظلّة محكمة «فيسا»: ملخّص».
Patriot Debates,

http://apps.americanbar.org/natsecurity/patriotdebates/section-206

24. أثار ديفيد ليون تلك النقطة. ديفيد ليون (2003) «الرقابة بعد 11/9».
Polity,
http://www.polity.co.uk/book.asp?ref=0745631819.

25. مجلة سكاي مول. «بريك هاوس سيكيوريتي» (2014). مقال: «أداة التجسّس على «آي فون» / «أندرويد»».
Skymall,
https://www.skymall.com/iphone-%2F-android-spy-stick/28033GRP.html

26. «كي لوغرز. كوم» (2014). مقال: «أفضل مسجّلات المفاتيح: مقارنة ومراجعة».
http://www.keyloggers.com

27. «الجني الخفي» (2014). «اعتراض المكالمات الجارية».
http://www.stealthgenie.com/features/live-call-intercept.html

28. موقع «آمازون. كوم» (2014). «دي جي آي فانتوم 2 مستعد لإطلاق هليكوبتر رباعيّة- مع «زنميوز آتش 3 كاميرا ثنائيّة الأبعاد، «غيمبال»: 959$ (في القائمة 999$)».
Amazon.com,
http://www.amazon.com/Dji-Phantom-Ready-Fly-Quadcopter/dp/B00H7HPU54

29. هنالك نماذج أوليّة عن مجسّات طائرة لها هيئة العصافير والحشرات، بل ربما أصغر- تقارب نثار الغبار- تحلق مع الريح. إليزابيث بوميلر وتوم شانكر (19 يونيو 2013). صحيفة نيويورك تايمس، مقال: «الحرب تتطوّر مع الـ«درون» وأدوات تشبه الحشرات».
New York Times,
http://www.nytimes.com/2011/06/20/world/20drones.html.
جون دبليو وايتهيد (15 إبريل 2013). «صراصير وبعوض وعصافير: الثورة المقبلة في الـ«ميكرو- درون»».
Rutherford Institute,
https://www.rutherford.org/publications_resources/john_whiteheads_commentary/roaches_mosquitoes_and_birds_the_coming_micro_drone_revolution

30. آشكان سلطاني (9 يونيو 2014). مقال: «تكلفة الرقابة».
http://ashkansoltani.org/2014/01/09/the-cost-of-surveillance
كيفن إس. بانكستون وآشكان سلطاني (9 يناير 2014). «ضباط بأحجام ضئيلة وتكلفة الرقابة: مراكمة سنتات من المواجهة بين الولايات المتحدة والمجرمين المجهولين».
Yale Law Journal 123,
http://yalelawjournal.org/forum/tiny-constables-and-the-cost-of-surveillance-making-cents-out-of-united-states-v-jones.

31. كاري جونسون (21 مارس 2012): «الـ«إف بي آي» تصارع قضائياً بشأن أحكام عن الـ«جي بي إس»».
NPR Morning Edition,
http://www.npr.org/2012/03/21/149011887/fbi-still-struggling-with-supreme-courts-gps-ruling

32. شون موسغريف (5 مارس 2014): «شبكة ضخمة للرقابة تجتاح أميركا بدفع من تجارة إعادة الامتلاك».
BetaBoston/Boston Globe, http://betaboston.com/news/2014/03/05/a-vast-hidden-surveillance-networkruns-across-america-powered-by-the-repo-industry
شون موسغريف (5 مارس 2014): «قاعدة بيانات مكثّفة عن اللوحات المعدنيّة للمركبات تشبه «إنستغرام»، وفق ما تشدّد عليه «شبكة التعرّف الإلكتروني»».
BetaBoston/Boston Globe,
http://betaboston.com/news/2014/03/05/massive-license-plate-location-database-just-like-instagram-digital-recognition-network-insists

33. «فيجيلانت فيديو» (23 فبراير 2009): «وثيقة إعداديّة مختصّة بالمواقع ومعدّة للتثبيت في خوادم «ليرن 4.0».

https://www.aclu.org/files/FilesPDFs/ALPR/texas/alprpra_portharthurPD_portarthurtx%20%287%29.pdf.

34. سايروس فاريفار (27 فبراير 2012): «سيارتك ملاحقة: الصعود السريع لظاهرة القارئات الضوئيّة للوحات المعدنيّة».

Ars Technica,

http://arstechnica.com/tech-policy/2012/09/your-car-tracked-the-rapid-rise-of-license-plate-readers

كاثرين كرامب (18 يوليو 2013). «الاتحاد الأميركي للحريّات المدنيّة»، «هناك من يتتبعّك: كيف استخدمت القارئات الضوئيّة للوحات المعدنيّة في تعقّب تحرّكات الأميركيين».

American Civil Liberties Union,

https://www.aclu.org/files/assets/071613-aclu-alprreport-opt-v05.pdf

35. كريغ تيمبرغ وإلين ناكاشيما (16 يونيو 2013). صحيفة واشنطن بوست. مقال: «قواعد بيانات صور بطاقات الهويّة تحوّلت إلى كنوز للبوليس».

Washington Post,

www.washingtonpost.com/business/technology/state-photo-id-databases-become-troves-for-police/2013/06/16/6f014bd4-ced5-11e2-8845-d970ccb04497_story.html.

36. جوش هيكز (18 فبراير 2014). صحيفة واشنطن بوست. مقال: «وزارة الأمن الوطني تريد صنع قاعدة بيانات موحّدة استناداً إلى القارئات الضوئيّة للوحات المعدنيّة للمركبات».

Washington Post,

http://www.washingtonpost.com/blogs/federal-eye/wp/2014/02/18/homeland-securitywants-to-build-national-database-using-license-plate-scanners.

دان فرومكين (17 مارس 2014) «تقارير عن موت قاعدة بيانات وطنيّة لتعقّب اللوحات المعدنيّة».

Intercept,

https://firstlook.org/theintercept/2014/03/17/1756license-plate-tracking-database.

37. جيمس بريدل (18 ديسمبر 2013): «كيف استوردت المملكة المتحدة جيل المستقبل للرقابة».

Medium,

https://medium.com/matter-archive/how-britain-exported-next-generation-surveillance-d15b5801b79e.

جنيفر لينش وبيتر بيبرنغ (6 مايو 2013). «مؤسّسة الحدود الإلكترونيّة»، مقال: «القارئات الضوئيّة المؤتمتة للّوحات المعدنيّة تهدد خصوصيّتنا».

Electronic Frontier Foundation,

https://www.eff.org/deeplinks/2013/05/alpr.

38. تحصل الشرطة على تلك البيانات أيضاً. هيلين موهيلاند (2 أبريل 2012)، صحيفة الغارديان، مقال: «بوريس جونسون يخطّط لمنح الشرطة نفاذاً إلى كاميرات مراقبة المرور».

Guardian,

http://www.theguardian.com/politics/2012/apr/02/boris-johnson-policecongestion-charge.

39. دان فرومكين (17 مارس 2014): «مبالغة كبرى في التقارير عن موت قاعدة بيانات وطنيّة عن اللوحات المعدنيّة للمركبات».

Intercept,

https://firstlook.org/theintercept/2014/03/17/1756license-plate-tracking-database

40. مكتب الـ«إف بي آي» (15 سبتمبر 2014): «الـ«إف بي آي» تعلن امتلاك قدرة عملانيّة للجيل المقبل من نظام التعرّف».
http://www.fbi.gov/news/pressrel/press-releases/fbi-announces-full-operationalcapability-of-the-next-generation-identification-system

41. وليام ماكلين (2 أكتوبر 2014). وكالة «رويترز». مقال: «مفتّشو دبي يحصلون على نظارات «غوغل» لمكافحة الجريمة».
Reuters,
http://www.reuters.com/article/2014/10/02/us-emirates-dubai-google-police-idUSKCN0HR0W320141002

42. غلين غرينوالد (5 يونيو 2013). صحيفة الغارديان، مقال: «تجمع «وكالة الأمن القومي» سجلات المكالمات ملايين من زبائن «فريزون» يومياً».
Guardian,
http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order

43. براندون كريغ (20 أغسطس 2013). شبكة «سي آن آن». «خرائط جديدة من «غوغل» تمكّنك من تجنّب ازدحام الطرق».
CNN,
http://www.cnn.com/2013/08/20/tech/mobile/google-waze-mobile-maps

44. آلكساندرا ألتر (19 يوليو 2012). صحيفة وول ستريت جورنال. مقال: «قارئك الإلكتروني يقرؤك».
Wall Street Journal,
http://online.wsj.com/news/articles/SB10001424052702304870304577490950051438304

45. ينطبق الوصف عينه على مشاهدتك لأشرطة الفيديو في «نتفلكس»، «آمازون»، «هولو» أو أي موقع لخدمة توجيه أشرطة الفيديو.

46. جنيفر لي (21 مارس 2002). صحيفة نيويورك تايمس. «نرحب بكم في ردهة قواعد البيانات».
Jennifer 8. Lee (21 Mar 2002),«Welcome to the database lounge,» *New York Times,* http://www.nytimes.com/2002/03/21/technology/welcome-to-the-database-lounge.html
Katie R. Holloman and D. Evan Ponder (2007), «Clubs, bars, and the driver's license scanning system,» in *Privacy in a Transparent World,* ed. Amy Albert, Ethica Publishing, http://www.ethicapublishing.com/7CH5.htm.

47. «بازفييد» (10 إبريل 2014). «ما مدى حظوتك الاجتماعيّة؟»
http://www.buzzfeed.com/regajha/how-privileged-are-you

48. كايتلين ديوي (24 يونيو 2014). صحيفة واشنطن بوست. مقال: «الحقيقة المذعرة التي يجب أن تفتح العيون على التتبّع في الإنترنت- عن الامتحانات القصيرة في موقع «بازفييد» وغيره».
Washington Post,
http://www.washingtonpost.com/news/the-intersect/wp/2014/06/26/the-scary-eye-opening-truth-of-internet-tracking-on-buzzfeed-quizzesand-everywhere-else

49. ماركو دي. هويشه (28 أكتوبر 2013): «تهديد الخصوصيّة أثناء البحث عن معلومات صحيّة».
JAMA Internal Medicine,
http://archinte.jamanetwork.com/article.aspx?articleid=1710119

50. رون نيكسون (3 يوليو 2013). صحيفة نيويورك تايمس. مقال: «تقدّم «هيئة البريد في الولايات المتحدة» البريد كلّه إلى قوى إنفاذ القانون».
New York Times,
http://www.nytimes.com/2013/07/04/us/monitoring-of-snail-mail.html

51. إم إس سـميث (18 يونيو 2012). «نتورك وورلد». مقال: «مسـتقبل الرقابة بالـ«درون»: حشرة سايبورغيّة تكون «درون»».
Network World,
http://www.networkworld.com/article/2222611/microsoft-subnet/the-future-of-drone-surveillance--swarms-of-cyborg-insect-drones.html.

52. رافي سوبان وداتاترياي مانكايم (2014): «المؤشّرات البيومتريّة في التعرّف إلى الوجوه: تحليل ومراجعة».
*Recent Advances in Intelligent Informatics: Advances in Intelligent Systems and Computing*235,
http://link.springer.com/chapter/10.1007%2F978-3-319-01778-5_47

53. تشـاو تشـاو لو وإكزايو تانغ (15 إبريل 2014): «التفوّق على القدرة البشريّة في التأكّد من الوجوه بواسـطة الوجوه المرسومة إحصائيّاً».
«Surpassing human-level face verification performance on LFW with GaussianFace,»
arXiv:1404.3840 [cs.CV],
http://arxiv.org/abs/1404.3840

54. باري فوكس (5 فبراير 2007). مجلة نيوسـاينتست. مقال: «ابتكار: جهاز خفي لمسح القزحيّة».
New Scientist,
http://www.newscientist.com/article/dn11110-invention-covert-iris-scanner.html

55. 133 زهاوزيانغ زانغ وماودي هو ويونغ هونغ وانغ. (2011). «مسح استقصائي عن التقدّم في التعرّف إلى طريقة المشي بالمؤشّرات البيومتريّة».
Biometric Recognition, Lecture Notes in Computer Science 7098, Springer-Verlag,
http://link.springer.com/chapter/10.1007%2F978-3-642-25449-9_19

56. كاثرين آلبريشـت (2008). مجلة ساينتيفك أميركان (سـبتمبر 2008)، مقال: «مؤشّرات نظام «رفيد»: أنه هويّتك».
72–77,
http://www.scientificamerican.com/article/how-rfid-tags-could-be-used.
University of Washington College of Engineering (22Feb 2008), «University launches RFID people tracking experiment,» *RFID Journal,*
http://www.rfidjournal.com/articles/view?6924
كريسـتوفر زارا (8 يناير 2013). انترناشيونال بيزنس تايمس، مقال: «سوار يعمل بنظام «رفيد» كأنه آتٍ من عوالم «ديزني»، وهو يشكّل منحدراً خطراً وفق نشطاء الخصوصيّة».
International Business Times,
http://www.ibtimes.com/disney-worlds-rfidtracking-bracelets-are-slippery-slope-warns-privacy-advocate-1001790.

57. كوانتـين هاردي (7 مـارس 2013)، صحيفة نيويورك تايمس، مقال: «التقنيّة تركز على تعقّب الناس خارج الإنترنت».
New York Times,
http://bits.blogs.nytimes.com/2013/03/07/technology-turns-to-tracking-people-offline.

58. سـتيفاني كليفـورد وكوانتين هاردي (15 يوليـو 2013)، صحيفة نيويـورك تايمس، مقـال: «انتبهوا أيها المتبضعون: المخزن يتعقّب هاتفكم الخلوي».
New York Times,
http://www.nytimes.com/2013/07/15/business/attention-shopper-stores-are-tracking-your-cell.html
برايان فانغ (19 أكتوبر 2013). صحيفة واشـنطن بوسـت. مقال: «كيف تستعمل المخازن الكبرى الـ«واي فاي» في هواتفكم كي تتعقّب عاداتكم في التبضّع».
Washington Post,

http://www.washingtonpost.com/blogs/the-switch/wp/2013/10/19/how-stores-use-your-phones-wifi-to-track-your-shopping-habits

لاتانيا سويني (12 فبراير 2014). مقال: «هاتفي في خدمتك». «اللجنة الفيدرالية للتجارة في الولايات المتحدة».
US Federal Trade Commission,

http://www.ftc.gov/news-events/blogs/techftc/2014/02/my-phone-your-service

59. بران بون وآخرون (4-7 يونيو 2013). «استعمال الإحصاء وموجات الـ«واي فاي» في التتبّع اللاإرادي للناس أثناء المناسبات العامة».

14th International Symposium and Workshops on World of Wireless, Mobile and Multimedia Networks,Madrid,

http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=6583443

60. كورت مغلبي (3 فبراير 2014)، «رسالة إلى المحترم آل فرانكين، مجلس الشيوخ الأميركي»، طلب جواب بشأن تجميع المعلومات محليّاً.

http://www.franken.senate.gov/files/letter/140212FordResponse.pdf.

61. «مكتب موثوقيّة الحكومة» (6 ديسمبر 2013)، «خدمات مستندة إلى جمع بيانات من السيّارات: الشركات تتخذ خطوات بشأن الخصوصيّة، لكن بعض المخاطر ليس واضحاً للزبائن»، تقرير إلى رئيس اللجنة الفرعيّة عن الخصوصيّة والتكنولوجيا والقانون، اللجنة التشريعيّة، مجلس الشيوخ.

GAO-14-81,

http://www.gao.gov/products/GAO-14-81

62. هيئة الـ«بي بي سي» (10 مارس 2008)، «كاميرا «تنظر» بواسطة الملابس».

BBC News,

http://news.bbc.co.uk/2/hi/technology/7287135.stm

روكو باراسكاندولا (23 يناير 2013)، صحيفة نيويورك تايمس، مقال: «مفوّض قسم شرطة نيويورك يصرح بأنّ القسم يختبر قريباً أداة تقنية متقدّمة جديدة تستطيع كشف الأسلحة المخبّأة».

New York Daily News,

http://www.nydailynews.com/new-york/nypdreadies-scan-and-frisk-article-1.1245663

كارتر إم. أرمسترونغ (17 أغسطس 2012)، «الحقيقة حول رادار الـ«تيراهرتز».

IEEE Spectrum,

http://spectrum.ieee.org/aerospace/military/the-truth-about-terahertz

63. لاري هاردستي (4 أغسطس 2014)، «إم آي تي نيوز»، مقال: «استخراج الأصوات من البيانات البصريّة».

MIT News,

http://newsoffice.mit.edu/2014/algorithm-recovers-speech-from-vibrations-0804

آبي ديفيس وآخرون (10- 14 أغسطس 2014)، «الميكروفون البصري: الاستخراج السلبي للصوت بواسطة أشرطة الفيديو».

41st International Conference on Computer Graphics and Interactive Techniques (SIGGRAPH 2014), Vancouver, British Columbia,

http://people.csail.mit.edu/mrub/papers/VisualMic_SIGGRAPH2014.pdf.

64. إريك كين (30 ديسمبر 2013). مجلة فوربس، مقال: «تقارير عن قدرة «وكالة الأمن القومي» على النفاذ إلى هواتف «آبل- آي فون»».

Forbes,

http://www.forbes.com/sites/erikkain/2013/12/30/the-nsa-reportedly-has-total-access-to-your-iphone

65. شاون ووترمان (9 مارس 2009)، وكالة أنباء «يو بي آي»، مقال: «وزارة الأمن الوطني تريد استعمال رائحة الجسم البشري كمعرّف بيومتري ومؤشّر للخداع».

UPI,

http://www.upi.com/Top_News/Special/2009/03/09/DHS-wants-to-use-human-body-odoras-biometric-identifier-clue-to-deception/UPI-20121236627329.

66. براناف ديكيست (19 أغسطس 2014)، مجلة جزمودو، مقال: «البنوك باتت تتعرف إليك من طريقة طباعتك».

Gizmodo,
http://gizmodo.com/your-phonecan-now-identify-you-based-on-how-you-type-1623733346

67. يسمّى ذلك «المؤشّر الأسلوبي». ساديا أفروز وفريقها. (18-21 مايو 2014). ورقة بحث: «مكتشف الشبيه الشبحي: استعمال المؤشّر الأسلوبي خفية».

IEEE Symposium on Security & Privacy, Oakland, California,
http://www.cs.gmu.edu/~mccoy/papers/oakland2014-underground.pdf.

68. رفائيل ساتر (13 أكتوبر 2014). «وكالة أسوشيتدبرس». مقال: «حصد بصمات الصوت بالملايين».
Associated Press,
http://www.washingtonpost.com/business/technology/millions-of-voiceprints-quietly-being-harvested/2014/10/13/b34e291a-52af-11e4-b86d-184ac281388d_story.html

رفائيل ساتر (13 أكتوبر 2014). «وكالة أسوشيتدبرس». مقال: «البنوك تحصد بصمات المكالمات بهدف مكافحة الفساد».

Associated Press,
http://www.washingtonpost.com/world/europe/banks-harvest-callers-voiceprints-tofightfraud/2014/10/13/715c6e56-52ad-11e4-b86d-184ac281388d_story.html.

69. نيكولا كلارك (17 مارس 2014). صحيفة نيويورك تايمس، مقال: «خطوط الطيران تستعمل التقنيّات الرقميّة كي تُضحي شخصيّة أكثر».

New York Times,
http://www.nytimes.com/2014/03/18/business/airlines-use-digital-technology-to-get-even-more-personal.html.

70. أندرو هويف (10 مارس 2010). صحيفة التلغراف، مقال: «[من وحي فيلم] «تقرير الأقليّة»: لوحات الإعلان تراقب زبائن المحلات».

Telegraph,
http://www.telegraph.co.uk/technology/news/7411249/Minority-Report-digital-billboard-watches-consumers-shop.html.

71. كلينت بولدن (11 أكتوبر 2013)، صحيفة وول ستريت جورنال [بلوغز]، مقال: «صُنّاع أطعمة الـ«سناك» يحدّثون مستويات الشراء بواسطة المجسّات وأدوات التحليل الرقميّة».

Wall Street Journal Blogs,
http://blogs.wsj.com/cio/2013/10/11/snackmaker-modernizes-the-impulse-buywith-sensors-analytics.

72. هناك فيلم خيال علمي يعرض تلك الأفكار بشكل ممتاز. كين ليو (ديسمبر 2012)، مجلة لايت سبيد، مقال: «التطابق الكامل».

Lightspeed Magazine,
http://www.lightspeedmagazine.com/fiction/the-perfect-match

73. برايان أكوهايدو (15 نوفمبر 2011)، صحيفة يو إس إيه توداي، مقال: «التدقيق في رقابة «فيسبوك».
USA Today,
http://usatoday30.usatoday.com/tech/news/story/2011-11-15/facebook-privacy-tracking-data/51225112/1

74. كوتون ديلو (22 فبراير 2013): «شراكة «فيسبوك» مع شركة «أكزيكوم»، وشركة «إيبسلون» تقابل مشتريات المحلات مع بروفايلات مستخدميها».

Advertising Age,

http://adage.com/article/digital/facebook-partner-acxiom-epsilon-match-storepurchases-user-profiles/239967

75. أحاول استخدام محرّك البحث «داك داك غو» الذي لا يجمع بيانات شخصيّة عن مستخدميه.
https://duckduckgo.com.

76. جوناثان ماير (17 فبراير 2012)، ويب بوليسي، مقال: أدوات التعقّب في محرّك البحث «سفاري».
Web Policy,
http://webpolicy.org/2012/02/17/safari-trackers.

77. بنجامين ماكو هيل (11 مايو 2014). مقال: «يملك «غوغل» معظم بريدي لأنه يملك بريدك كلّه».
Copyrighteous,
http://mako.cc/copyrighteous/google-has-most-of-my-email-because-it-has-all-of-yours

78. مون مونغ (4 مايو 2011)، مقال: «المُدُن الخمسة الأولى في ضخامة الشبكات المخصّصة لكاميرات المراقبة».
VinTech Journal,
http:// www.vintechnology.com/journal/uncategorized/top-5-cities-with-the-largestsurveillance-camera-networks

ديفيد باريت (10 يوليو 2013)، صحيفة التلغراف، مقال: «كاميرا مراقبة لكل 11 شخصاً شخص في لندن، وفق مسح إحصائي لـ«سي سي تي في»».

Telegraph,
http://www.telegraph.co.uk/technology/10172298/One-surveillance-camera-for-every-11-people-in-Britain-says-CCTV-survey.html.

مجموعة «ثالث»، (11 إبريل 2014)، «مدينة مكسيكو بوصفها تمثّل الطموح الأضخم لبرامج الأمن الحضري».
https://www.thalesgroup.com/en/worldwide/security/case-study/mexico-city-worlds-most-ambitious-urban-security-programme.

79. شركة «سي غايت تكنولوجيز» (2012)، «تخزين أشرطة الرقابة: ما هو الحدّ الكافي»؟
http://m.seagate.com/files/staticfiles/docs/pdf/whitepaper/video-surv-storage-tp571-3-1202-us.pdf

80. جيرمي بِنثام (1791)، كتاب **البان أوبتيكون أو منزل- التفتيش**. دار النشر «تي. باين».
http://cartome.org/panopticon2.htm

81. أوسكار إتش غاندي جونيور (1993)، كتاب **نوع البان أوبتيكون: الاقتصاد السياسي للمعلومات الشخصيّة**، دار «ويست فيو برس».
http://books.google.com/books?id=wreFAAAAMAAJ.

82. توم برينغال الثالث (2002). كتاب: **البان أوبتيكون الجديد: الإنترنت بوصفها بنية للسيطرة الاجتماعيّة**. «جامعة تينيسي للتكنولوجيا».
http://unpan1.un.org/intradoc/groups/public/documents/apcity/unpan003570.pdf.

83. إلين ناكاشيما (16 يناير 2007). صحيفة **واشنطن بوست**. مقال: «التمتّع بتسهيلات التكنولوجيا، مع عدم النجاة من رقابتها اليقظة».

Washington Post,
http://www.washingtonpost.com/wp-dyn/content/article/2007/01/15/AR2007011501304.html

الفصل 3 : تحليل بياناتنا

1. تشارلز دو هيغ (16 فبراير 2012)، صحيفة نيويورك تايمس، مقال: «كيف تعرف الشركات أسرارك»؟
http://www.nytimes.com/2012/02/19/magazine/shopping-habits.html.

2. غريغوري بياتسكي (8 ديسمبر 2013). مقال: «المراحل الثلاث للبيانات الضخمة».
KD Nuggets,
http://www.kdnuggets.com/2013/12/3-stages-big-data.html.

3. ميتشيل شراير (7 نوفمبر 2012)، مجلة تايم، مقال: «جولة في عالم ملتهمي المعلومات الذين ساعدوا في فوز أوباما».
Time,
http://swampland.time.com/2012/11/07/inside-the-secret-world-of-quants-and-data-cruncherswho-helped-obama-win

4. أقدّم مثلين عن ذلك. لارس باكستورم وآخرون (5 يناير 2012). «أربع درجات من الانفصال».
arXiv:1111.4570 [cs.SI],
http://arxiv.org/abs/1111.4570.
راسل ب. كلايتون (يوليو 2014). مقال: «الدولاب الثالث: أثر استخدام «تويتر» في الخيانة الزوجيّة والطلاق».
*Cyberpsychology, Behavior, and Social Networking*17,
http://www.cs.vu.nl/~eliens/sg/local/cyber/twitter-infidelity.pdf.

5. تمكّنت تجربة من التمييز بين الرجال المثليّين وغيرهم في 88 % من الحالات، وبين الأفارقة الأميركيّين ونظرائهم البيض في 95 % من الحالات، وبين الديمقراطيّين والجمهوريّين في 85 % من الحالات. ميشال كوزنسكي، ديفيد ستلويل، وثور غرايبل (11 مارس 2013)، دراسة: «الخصائص والانتماءات الشخصيّة قابلة للتوقع من السجلات الرقميّة».
Proceedings of theNational Academy of Sciences of the United States of America, Early Edition, http://www.pnas.org/content/early/2013/03/06/1218772110.

6. سارة م. واتسون (14 مارس 2012)، مجلة آتلانتيك، مقال: «لم أخبر «فيسبوك» بخطوبتي، فلماذا يسألني عن خطيبي»؟
Atlantic,
http://www.theatlantic.com/technology/archive/2012/03/i-didnt-tell-facebook-im-engagedso-why-is-it-asking-about-my-fianc/254479.

7. كاتي هايني (19 مارس 2013). مقال: «عرف «فيسبوك» أنني مثليّ جنسيّاً قبل أن تعرف عائلتي بذلك».
BuzzFeed,
http://www.buzzfeed.com/katieheaney/facebookknew-i-was-gay-before-my-family-did

8. جيفري أ. فاولار (13 أكتوبر 2012). صحيفة وول ستريت جورنال، مقال: «عندما يعلن «فيسبوك» على الملأ، الأسرار الأكثر حميميّة».
Wall Street Journal,
http://online.wsj.com/news/articles/SB100008723963904441658045780087405 78200224

9. في فترة ما من العام 2014، تضمّن تطبيق «غرندر» (Grindr) المخصّص للمثليّين، معلومات تمكن من الوصول إلى كل مثليّ جنسيّاً في العالم، بما في ذلك بلدان كأوغندا وروسيا وإيران. جون آرافوسس (26 أغسطس 2014)، مقال: «تطبيق «غرندر» الشائع بين مثليّي الجنس يواجه اختراقات أمنيّة مريبة».
America Blog,
http://americablog.com/2014/08/grindr-users-unwittingly-giving-away-exact-location.html.

10. سارة م. واتسون (16 سبتمبر 2014). قناة «الجزيرة» وموقعها الإلكتروني. مقال: «اسأل جهاز فك تشفير قنوات التلفزيون: التربص بالضربات».

Al-Jazeera,
http://america.aljazeera.com/articles/2014/9/16/the-decoder-stalkedbysocks.html

11. سيلفان لاين (13 أغسطس 2014). «الإعلانات الـ16 الأكثر إثارة للريبة على «فيسبوك»».
Mashable,
http://mashable.com/2014/08/13/facebook-ads-creepy.

12. غاي غغليوتا (19 يونيو 2006). صحيفة واشنطن بوست. مقال: «التنقيب في البيانات ما زال بحاجة إلى توجيه ليكون فعّالاً».
Washington Post,
http://www.washingtonpost.com/wp-dyn/content/article/2006/06/18/AR2006061800524.html

فيليب سيغال (28 مارس 2011). مقال: «التنقيب في المعلومات ذكاء يسير بغباء».
Ethical Investigator,
http://www.ethicalinvestigator.com/internet/data-mining-is-dumbed-down-intelligence.

أوغي أوغاس (8 فبراير 2013). مجلة وايرد، مقال: «احذر من الأخطاء الضخمة في البيانات الضخمة».
Wired,
http://www.wired.com/2013/02/big-data-means-big-errors-people.

13. بارتون غيلمان وآشكان سلطاني (18 مارس 2014). صحيفة واشنطن بوست. «برنامج الرقابة في «وكالة الأمن القومي» يصل إلى الماضي، ويستعيد المكالمات الهاتفيّة ويشغّلها».
Washington Post,
http://www.washingtonpost.com/world/national-security/nsa-surveillance-program-reaches-into-the-past-to-retrieve-replay-phone-calls/2014/03/18/226d2646-ade9-11e3-a49e-76adc9210f19_story.html.

14. وزارة العدل الأميركيّة. (16 ديسمبر 2009). «وافق بنك «كريدي ليونيه» على دفع غرامة بـ 536 مليون دولار تتعلّق باختراقه «قانون الأحوال الطارئة لقوى الماليّة الدوليّة» وقانون مقاطعة نيويورك».
http://www.justice.gov/opa/pr/2009/December/09-ag-1358.html.

مكتب المدّعي العام لمقاطعة نيويورك (10 ديسمبر 2012). «بنك «ستاندرد شارتر يقبل دفع 327 مليون دولار غرامة عن معاملات غير قانونيّة».
http://manhattanda.org/node/3440/print

مكتب المدعي العام لمقاطعة نيويورك (30 حزيران 2014). «بنك «بي أن بي باري باه» يقر بأنّه مذنب، ويقبل بدفع 8.83 بليون دولار غرامة عن معاملات غير قانونيّة».
http://manhattanda.org/node/4884/print.

15. سكوت روزنفيلد (23 يوليو 2013). نتائج إيجابيّة [بوجود منشّطات] لثلاثة من أوائل الدرّاجين في مسابقة «تور دي فرانس».
Outside Online,
http://www.outsideonline.com/news-from-the-field/Top-3-Finishers-in-1998-Tour-Test-Positive.html

16. غلين غرينوالد (21 يوليو 2013). صحيفة الغارديان. مقال: «أداة «إكس كي سكور» لدى «وكالة الأمن القومي»، تجمع معظم ما يفعله جمهور الإنترنت».
Guardian,
http://www.theguardian.com/world/2013/jul/31/nsa-top-secret-program-online-data

«وكالة الأمن القومي» (8 يناير 2007) «إكس كي سكور» (شرائح صوتيّة تدريبيّة).
https://www.eff.org/document/2013-07-31-guard-xkeyscore-training-slides page 2.

17. جيمس بول (30 سبتمبر 2013)، صحيفة الغارديان، مقال: «قاعدة بيانات لدى «وكالة الأمن القومي» تحتفظ بالـ «ميتاداتا» لملايين مستخدمي الإنترنت لسنة، وفق ما تظهره ملفات سريّة».

Guardian,
http://www.theguardian.com/world/2013/sep/30/nsa-americans-metadata-year-documents

18. ريــان ديفيرو، غلين غرينوالد ولورا بيوتراس (19 مايــو 2014). «قراصنة البيانات في الكاريبي: «وكالة الأمن القومي» تسجّل المكالمات الخلوية كافة في الـ«باهاماس».

Intercept,
https://firstlook.org/theintercept/article/2014/05/19/data-pirates-caribbean-nsa-recording-every-cell-phone-call-bahamas

جوليان آســانج (23 مايو 2014)، «إعلان من «ويكيليكس» بصدد تســجيلات الهاتف الجماعيّة للأفغان، من قِبَل «وكالة الأمن القومي».

WikiLeaks,
https://wikileaks.org/WikiLeaks-statement-on-the-mass.html.

19. ديفيــد كرافتــس (17 يناير 2014)، مجلــة وايرد، مقال: أوباما يعيد هيكلة برنامــج «وكالة الأمن القومي» في التجسّس على الـ«ميتاداتا».

Wired,
http://www.wired.com/2014/01/obama-nsa.

20. لا أعرف إذا كان ذلك يشــمل الحوارات الشــبكيّة المشفّرة بطريقة «إس إس إل»، لكن يخامرني ظنٌّ بأن الوكالة تفكك (تلك) كثيراً من ذلك التشــفير في الوقت الحي. ماثيو غرين، (2 ديســبمر 2013)، مدوّنة إلكترونيّة، كيف تكسر «وكالة الأمن القومي» شيفرة الـ«إس إس إل»؟

A Few Thoughts on Cryptographic Engineering,
http://blog.cryptographyengineering.com/2013/12/how-does-nsa-breakssl.

21. بارتون غيلمان وآشكان سلطاني (4 ديسمبر 2013)، صحيفة واشنطن بوست. مقال: «تتعقّب «وكالة الأمن القومي» الهواتف في العالم كله».

Washington Post,
http://www.washingtonpost.com/world/national-security/nsa-tracking-cellphone-locations-worldwide-snowden-documents-show/2013/12/04/5492873a-5cf2-11e3-bc56-c6ca94801fac_story.html

22. جيمس بامفورد (15 مارس 2012)، مجلة وايرد، مقال: «وكالة الأمن القومي» تبني المركز الأضخم للتجسّس في البلاد (راقب ما تقوله)».

Wired,
http://www.wired.com/threatlevel/2012/03/ff_nsadatacenter/all.

23. كيفن بولسن (27 يناير 2014). مجلة وايرد، مقال: «إذا استخدمت هذا الموقع الآمن للبريد الإلكتروني، يحصل الـ«إف بي آي» على رسائلك».

Wired,
http://www.wired.com/2014/01/tormail.

24. ســايروس فاريفار (27 فبراير 2012)، مقال: «سيارتك ملاحقة: الصعود السريع لظاهرة الماسحات الضوئيّة للوحات المركبات». موقع «آرس تكنيكا».

Ars Technica,
http://arstechnica.com/tech-policy/2012/09/your-car-tracked-the-rapid-rise-of-license-plate-readers.

Steve Orr (26Jul 2014), «New York knows where your license plate goes,»
Democrat and Chronicle,
http://www.democratandchronicle.com/story/news/2014/07/26/new-york-licenseplate-readers/13179727.

25. ديـكلان ماكّولـه (19 مارس 2013). مقال: «رجال شرطة يطلبون أن يتضمن قانون الولايات المتحدة ما يتيح الحصول على سجلاتك الهاتفيّة». موقع «سي نت» للأخبار.
CNET,
http://news.cnet.com/8301-13578_3-57575039-38/cops-u.s-law-should-require-logs-of-your-text-messages.
على بُعد ثلاث «قفزات» من آليس. فيليب بوم (17 يوليو 2013)، آتلانتك واير، مقال: «وكالة الأمن القومي تقرّ بأنّها تحلل بيانات الناس بأكثر مما صرّحت عنه سابقاً».
Atlantic Wire,
http://www.thewire.com/politics/2013/07/nsa-admits-it-analyzes-more-peoples-data-previously-revealed/67287.
26. يكتـب جوناثان مايرز عن صعوبة تحليل تلك البيانات. جوناثان مايرز وباترك موشـلر (9 ديسـمبر 2013). الـ«ميتا» هاتف: القفزات الثلاث لـ«وكالة الأمن القومي».
Web Policy,
http://webpolicy.org/2013/12/09/metaphone-the-nsa-threehop.
27. آيمي دايفدسـون (16 ديسـمبر 2013). صحيفة نيويوركر. نظريّة الـ«دومينـو» افتراضيّاً: القاضي ليون في مواجهة «وكالة الأمن القومي».
New Yorker,
http://www..newyorker.com/news/amy-davidson/the-dominos-hypothetical-judge-leon-vsthe-n-s-a.
28. بارتـون غيلمـان ولورا بواتراس (10 يوليو 2013). صحيفة واشـنطن بوسـت. مقـال: «الشرائح الضوئيّة لـ«وكالة الأمن القومي» تشرح طريقة عمل برنامج «بريزم» لجمع البيانات».
Washington Post,
http://www.washingtonpost.com/wp-srv/special/politics/prism-collection-documents
29. شـاين هاريـس (17 يوليو 2013). مجلة فورين بوليسي، مقال: ثلاث درجـات من الانفصال تكفي لوضعك تحت رقابة «وكالة الأمن القومي».
Foreign Policy,
http://complex.foreignpolicy.com/posts/2013/07/17/3_degrees_of_separation_is_enough_to_have_you_watched_by_the_nsa.
30. طوني برادلي (17 يناير 2014). مجلة فوربس، مقال: «ما قاله الرئيس أوباما ولم ينفّذه».
Forbes,
http://www.forbes.com/sites/tonybradley/2014/01/17/nsa-reform-what-president-obama-said-and-whathe-didnt.
31. جيمـس ريزن ولورا بواتراس (20 سـبتمبر 2013). صحيفة نيويورك تايمس، مقال: «وكالة الأمن القومي» تراقب العلاقات الاجتماعيّة للمواطنين الأميركيّين».
New York Times,
http://www.nytimes.com/2013/09/29/us/nsa-examines-social-networks-of-us-citizens.html
32. فوهيني فارا (23 أغسطس 2007)، صحيفة وول ستريت جورنال، مقال: «الانتقال إلى المشخصَن في إعلانات فيسبوك».
Wall Street Journal,
http://online.wsj.com/news/articles/SB118783296519606151
33. عندمـا تعثر «مايكروسـوفت» أو «غوغل» على أدلة عن جنـس أطفال إباحي، فإنها تبلـغ الشرطة عنك. ماثيو سـباركس (4 أغسـطس 2014)، صحيفة التلغراف، مقال: «لماذا يدقّق «غوغل» في بريدك بشأن جنس أطفال إباحي».
Telegraph,

http://www.telegraph.co.uk/technology/google/11010182/Why-Google-scans-your-emails-forchild-porn.html.

ليو كليون (6 أغسطس 2014). هيئة «بي بي سي»، مقال: «مؤشّرات من «مايكروسوفت» أدّت إلى اعتقالات في «بنسلفانيا» بشأن جنس أطفال إباحي».

BBC News,

www.bbc.co.uk/go/em/fr/-/news/technology-28682686

34. أشار «مجلس الإشراف على الخصوصيّة والحريّات المدنيّة» إلى أن تجميع «وكالة الأمن القومي» للبيانات تحت البند 702 من «قانون إصلاحات محكمة «فيسا»، لا ينطبق تجميع أسس الكلمات المفتاحيّة، على الرغم من كونه صلاحية منفردة، ما يعني وجود مساحة للتلاعب. «مجلس الإشراف على الخصوصيّة والحريّات المدنيّة» (2 يوليو 2014).

«Report on the surveillanceprogram operated pursuant to Section 702 of the Foreign Intelligence SurveillanceAct,»

http://www.pclob.gov/All%20Documents/Report%20on%20the%20Section%20702%20Program/PCLOB-Section-702-Report.pdf.

جنيفر غرانيك (11 فبراير 2014)، «ثمانية أسئلة من «مجلس الإشراف على الخصوصيّة والحريّات المدنيّة» بشأن البند 207».

Just Security,

https://justsecurity.org/7001/questions-pclob-section-702

35. جاكوب آبلبوم (3 يوليو 2014). مقال: «وكالة الأمن القومي تستهدف الأشخاص المتنبّهين للخصوصيّة».

Panorama,

http://daserste.ndr.de/panorama/aktuell/nsa230_page-1.html.

36. مارسي ويلر (15 نوفمبر 2013). موقع «إيمبتي ويل». مقال: «عن رأي محكمة «إف أي أس سي» في مايو 2007».

Empty Wheel,

http://www.emptywheel.net/2013/10/15/aboutthat-may-2007-fisc-opinion

37. مارسي ويلر (16 مايو 2014). موقع «إيمبتي ويل»، مقال: «عملية البحث المؤتمتة ستشمل روابط».

Empty Wheel,

http://www.emptywheel.net/2014/05/16/the-automated-query-at-the-telecoms-will-include-correlations.

مارسي ويلر (28 يونيو 2014). موقع «إيمبتي ويل»، مقال: «العملية المحسّنة الجديدة لـ«وكالة الأمن القومي» في ربط سلاسل المكالمات؛ لا تتطلّب حدوث اتصالات هاتفيّة».

Empty Wheel,

http://www.emptywheel.net/2014/06/28/nsas-new-and-improved-call-chaining-process-now-with-no-calls-required.

38. يحمل البرنامج اسماً شيفريّاً هو «كوترافلر» (CO- TRAVELLER). بارتون غيلمان وآشكان سلطاني (4 ديسمبر 2013). صحيفة واشنطن بوست. مقال: «وفق وثائق سنودن، «وكالة الأمن القومي» تتبّع مواقع الخلويات عالميّاً».

Washington Post,

http://www.washingtonpost.com/world/national-security/nsa-tracking-cellphone-locations-worldwide-snowdendocuments- show/2013/12/04/5492873a-5cf2-11e3-bc56-c6ca94801fac_story.html.

39. إدارة «وكالة الأمن القومي» (2012). «ملخّص عن الأدوات التحليليّة في برنامجيّ «دي آن آر» و«كوترافلر»».
https://www.eff.org/files/2013/12/11/20131210-wapo-cotraveler_overview.pdf.

40. جوليان سانشير (11 أكتوبر 2013). «جاست سيكيورتي». مقال: «استعمالات أخرى للقاعدة بيانات الهواتف لدى «وكالة الأمن القومي»: إيجاد بصمات أصحاب الهواتف «المحروقة»؟

Just Security,

http://justsecurity.org/2013/10/11/nsa-call-records-database-fingerprinting-burners

41. بارتون غيلمان وآشكان سلطاني (4 ديسمبر 2013). صحيفة واشنطن بوست. مقال: «وكالة الأمن القومي» تتعقّب الخلويات في العالم كله، وفق وثيقة من سنودن».

Washington Post,
http://www.washingtonpost.com/world/national-security/nsa-trackingcellphone-locations-worldwide-snowden-documents-show/2013/12/04/5492873a-5cf2-11e3-bc56-c6ca94801fac_story.html.

42. تمثّل تلك التقنية الأساسيّة في برنامج «كوترافلر». إذا كان هنالك هاتف يستخدم دوماً الشبكة التي يستعملها هاتف الرئيس، فالأرجح أنه في جيبك. وزارة العدل الأميركيّة (13 فبراير 2012). «شكوى جرميّة». الولايات المتحدة ضد جوزيه أغوييو وآخرون. (رقم القضية محظور).

United States District Court, Northern District of Illinois, EasternDivision,
http://www.justice.gov/usao/iln/pr/chicago/2013/pr0222_01d.pdf.

43. هياواثا براي (24 إبريل 2014). مجلة ديسكوفر. مقال: «كيف ترسم التطبيقات المستندة إلى الموقع الجغرافي مستقبل التبضّع».

Discover,
http://blogs.discovermagazine.com/crux/2014/04/30/how-location-based-apps-will-shape-the-future-of-shopping

44. لورين جونسون (9 يونيو 2014). «لماذا تعمل مايكروسوفت على نشر الإعلانات المستندة إلى الموقع الجغرافي عند مخازن البيع بالمفرق: الاختبارات أعلت شأن حركة المشاة». جريدة بوسطن غلوب.

Boston Globe,
http://www.bostonglobe.com/business/2013/07/07/your-cellphone-ourself/eSvTK1UCqNOE7D4qbAcWPL/story.html.

45. هياواثا براي (8 يوليو 2013).

Boston Globe,
http://www.bostonglobe.com/business/2013/07/07/your-cellphone-yourself/eSvTK1UCqNOE7D4qbAcWPL/story.html.

46. آلي وينستون (17 يونيو 2014). «مركز التقارير الاستقصائيّة». مقال: «خطط للتوسّع في أمدية القارئات الضوئيّة للوحات المركبات، وفق تحذير من محامين».

Center for Investigative Reporting,
http://cironline.org/reports/plans-expand-scope-licenseplate-readers-alarm-privacy-advocates-6451.

47. يناقش المقال التالي خطط الـ«إف بي آي» في فعل ذلك تحديداً. «مركز معلومات الخصوصيّة الإلكترونيّة» (ديسمبر 2013). «الجيل التالي من برامج الـ«إف بي آي» في التعرّف: نظام «الأخ الكبير» في الهويّة؟»

Spotlight on Surveillance,
https://epic.org/privacy/surveillance/spotlight/ngi.html.

48. برزت مخاوف بشأن استخدام بطاقات «أويستر» عندما ظهرت تلك التقنية في لندن سنة 2003. هيئة «بي بي سي». آرون شيليون (25 سبتمبر 2003) مقال: «بطاقة ذكيّة تتعقّب مستخدميها».

BBC News,
http://news.bbc.co.uk/2/hi/technology/3121652.stm.

49. غريغ ويستون، غلين غرينوود وراين غالاهار (30 يناير 2014). تلفزيون «سي بي سي نيوز». مقال: «وكالة «سيسك» استخدمت الـ«واي فاي» في المطار لتتبّع مسافرين كنديّين، وفق وثائق سنودن».

CBC News,
http://www.cbc.ca/news/politics/csecused-airport-wi-fi-to-track-canadian-travellers-edward-snowden-documents-1.2517881.

50. أليســاندرو آكويزتــي، رالــف كــروس وفريد شــتوتزمان (4 أغســطس 2011). مقــال: «وجوه «فيســبوك»: الخصوصيّة في زمن الحقيقة المدعّمة رقميّاً».
Black Hat 2011, Las Vegas, Nevada,
http://www.heinz.cmu.edu/~acquisti/face-recognition-study-FAQ/acquisti-faces-BLACKHAT-draft.pdf

51. سكوت إللارت (7 ديسمبر 1999). «نُظُم ووسائل للمناقلة البيانات بين قواعد البيانات (5999937 أ)». «المكتب الأميركي للعلامات التجاريّة وبراءات الاختراع».
http://www.google.com/patents/US5999937

52. كوتون ديلو (22 فبراير 2013). مقال: ««فيســبوك» يتشارك مع برنامج «إيبسلون» من شركة «آكزيكوم»، في مطابقة قوائم الشراء في المخازن مع بروفايلات مستخدميه».
Advertising Age,
http://adage.com/article/digital/facebook-partner-acxiom-epsilon-match-storepurchases-user-profiles/239967.

53. كارولــين كوبر وكلير غوردون (2 إبريل 2014). الموقع الشــبكي لقناة «الجزيرة». مقال: «هناك من يربح من معلومات عن عاداتك في الشرب وأمراضك المنقولة جنسيّاً».
Al Jazeera,
http://america.aljazeera.com/watch/shows/america-tonight/articles/2014/4/2/the-people-makingmoneyoffyourdrinkinghabitsandstds.html.

54. ماكس فيشر (19 فبراير 2013). صحيفة واشــنطن بوســت. مقال: «الــهاكرز» الصينيّون كشفوا أنفسهم بدخولهم إلى حساباتهم الشخصيّة على «فيسبوك»».
Washington Post,
http:// www.washingtonpost.com/blogs/worldviews/wp/2013/02/19/chinese-hackers-outed-themselves-by-logging-into-their-personal-facebook-accounts

55. بول روبرتس (7 مارس 2012). «الثرثرات على الــويب»، وحوادث الســيّارات، وممارســة النســخ واللصق، زرعت بذور مأساة مونزيغر».
Threatpost,
http://threatpost.com/chats-carcrushes-and-cut-n-paste-sowed-seeds-lulzsecs-demise-030712/76298.

56. كريــس ســوغيان (13 نوفمبر 2012). مقــال: «الرقابة ودروس الأمن المســتقاة من فضيحة بــاولا بردويل». «الاتحاد الأميركي للحريّات المدنيّة».
American Civil Liberties Union,
https://www.aclu.org/blog/technology-and-liberty-national-security/surveillance-and-security-lessons-petraeus-scandal.

57. دان أوكــس (12 إبريل 2012)، صحيفة ســيدني هيرالد مورنينغ. مقال: «حال أعطى فيها «هاكر» جســماً من الأدلة».
Sydney Morning Herald,
http://www.smh.com.au/technology/technology-news/hacking-cases-body-of-evidence-20120412-1wsbh.html.

58. رونين برغمان وآخرون (17 يناير 2011) صحيفة دير شــبيغيل. مقال: «عيناً بعين: تفاصيل عملية الموســاد الإسرائيلي في دبي».
Der Spiegel,
http://www.spiegel.de/international/world/an-eye-for-an-eye-the-anatomy-of-mossad-sdubai-operation-a-739908.html.

59. بول أوم (13 أغســطس 2009). ورقة بحث: «وعد الخصوصيّة المكسور: في الاستجابة للفشل الذريع لتقنيّات إخفاء الهويّة».

UCLA Law Review 57,
http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1450006.

60. ميشـيل باربورو وتوم زيلر جونيور (9 أغســطس 2006). صحيفة **نيويورك تايمس**. مقال: «الكشــف عن هويّة صاحب عملية البحث رقم 4417749 على موقع «إيه أو آل»».

New York Times,
http:// www.nytimes.com/2006/08/09/technology/09aol.html.

61. آرافند نارايان وفيتالي شماتيكوف (18-20 مايو 2008). ورقة بحث: «كشف الهويّات المغفلة بطريقة مكينة استناداً إلى قواعد بيانات مبعثرة».

2008 IEEE Symposium on Security and Privacy, Oakland, California,
http://dl.acm.org/citation.cfm?id=1398064 and
http://www.cs.utexas.edu/~shmat/shmat_oak08netflix.pdf

62. ولغايات بحثيّة في منتصف التســعينيات من القرن الماضي، نشرت «لجنة الضمان في مجموعة ماساشوســتس» ملفات المستشــفيات لموظّفي الدولة بعد أن أزالت منها الأســماء والعناوين وأرقام الضمان الاجتماعي. وبرهنت عالمة الكومبيوتر لاتانيا ســويني، وكانت حينها طالبة موشــكة على التخرّج من «معهد ماساشوستس للتقنية»، أنها اســتطاعت كسر إغفال الهويّة في الملفات بربطها تواريخ الميلاد وأرقام مشــاريع البلدية من جهة، وقاعدة بيانــات لتســجيل الناخبين. لاتانيا ســويني (يونيــو 1997)، ورقة بحــث: «حبك التكنولوجيا والسياســة معاً لضمان السريّة».

Journal of Law, Medicine and Ethics 25,
http://onlinelibrary.wiley.com/doi/10.1111/j.1748-720X.1997.tb01885.x/abstract.

63. لاتانيا ســويني (2000). بحث: «المعلومات الديموغرافيّة البســيطة تكفي أحياناً للتعــرّف إلى هوية متفرّدة». جامعة «كارنيغي- ميلون». ورقة بحث رقم 3 بشأن بيانات الخصوصيّة.

Carnegie Mellon University, Data Privacy Working Paper 3,
http://dataprivacylab.org/projects/identifiability/paper1.pdf.

64. فيليــب غــول (30 أكتوبر 2006). ورقة بحث: «إعادة البحث في فــرادة المعلومات في البيانات الديموغرافيّة عن سكان الولايات المتحدة».

population,» 5th ACM
Workshop on Privacy in the Electronic Society (WPES'06), Alexandria, Virginia,
http://crypto.stanford.edu/~pgolle/papers/census.pdf

65. ميليسا غايمرك وفريقها (18 يناير 2013). مجلة **ساينس**، ورقة بحث: «التعرّف إلى الحمض النووي للأفراد استناداً إلى استدلال من اسم العائلة».

Science 339,
http://www.sciencemag.org/content/339/6117/321.abstract.

جون بوحنّون وآخرون. مجلة **ساينس**، ورقة بحث: «قواعد البيانات عن شجرة العائلة تكشف أسماء المتبرعين المغفلي الهويّة للحمض النووي».

Science 339,
http://www.sciencemag.org/content/339/6117/262.

66. آدم تانر (11 أكتوبر 2013). مجلة **فوربس**. مقال: «الغوص في البيانات يكشف هويّات المشاركين في البحوث الجنسيّة».

Forbes,
http://www.forbes.com/sites/adamtanner/2013/10/11/decoding-the-secrets-of-sex-data

67. آرافند نارايان وفيتالي شماتيكوف (يونيو 2010). بحث: «أوهام وخرافات «المعلومات المعرّفة بالهويّة»».
Communications of the ACM 53,
http://dl.acm.org/citation.cfm?id=1743558.

68. رايـان غالاهار (25 أغسـطس 2014). موقع «إنترسـبت». مقال: «محرّك الرقابة: كيـف صنعت «وكالة الأمن القومي» محرك بحثها السري المشابه لـ«غوغل»».
Intercept,
https://firstlook.org/theintercept/2014/08/25/icreach-nsa-cia-secret-google-crisscross-proton.

69. إيف آلكسندر دي مونتجوي وآخرون. (4 فبراير 2013). موقع «نايتشر». مقال: «متفرّد وسط الحشد: حدود الخصوصيّة في الحراك الإنساني».
Scientific Reports 3, Article 1376,
http://www.nature.com/srep/2013/130325/srep01376/full/srep01376.html.

70. لا أقصد القول باسـتحالة تجهيل هويّة مجموعة ما من البيانات، لكنني أقول إن ذلك صعب جداً ومن السـهل الوقوع في الخطأ بشأنه. إذ يعتقد كثيرون بأن استبدال بيانات حسّاسة بأرقام عشوائيّة، يكفي لحمايتها، لكن ذلك خطأ. ففي أغلب الأحيان، لا ينفع ذلك الإجراء كليّاً.

71. من المسـتطاع أن نضرب مثلًا بقوانين «وزارة الأمن الوطنـي». ماري إلين غالاهان (مارس 2012). **كتاب عن تأمين المعلومات المعرّفة بالشخصيّة**. وزارة الأمن الوطني في الولايات المتحدة.
http://www.dhs.gov/sites/default/files/publications/privacy/Guidance/handbookforsafeguardingsensitivePII_march_2012_webversion.pdf.

الفصل 4: تجارة الرقابة

1. كايسي هاوزر (16 أكتوبر 2013). موقع «غازيل». مقال: «استعمل تطبيق الـ«فلاش» للخداع أو التعامل».
Gazelle,
https://www.gazelle.com/thehorn/2013/10/16/use-yourflashlight-app-for-trick-or-treating

2. سيسـيليا غانغ (5 ديسمبر 2013). صحيفة **واشنطن بوست**. مقال: «تطبيق للـ«فلاش» يبقي في الظلام أنّه يتشارك في «البيانات المكانيّة».
Washington Post,
http://www.washingtonpost.com/business/technology/f lashlight-app-kept-users-inthe-dark-about-sharing-location-data-ftc/2013/12/05/1be26fa6-5dc7-11e3-be07-006c776266ed_story.html.

3. جيسـون هونـغ (30 نوفمـبر 2012). مقـال: «تحليـل عـن تطبيق «برايتسـت فـلاش لايت فـري» لهواتف الـ«آندرويد»».
Jason Hong's Confabulations,
http://confabulator.blogspot.com/2012/11/analysis-of-brightest-flashlight-free.html

4. «اللجنـة الفيدراليّـة للتجارة» (5 ديسـمبر 2013). ورقة: «مطوّر تطبيق «فلاش لايت» للـ«آندرويد» يسـوّي اتّهامات «لجنة التجارة الفيدراليّة» بأنّه خدع المسـتهلكين: «برايتسـت فلاش» تشـارك بيانات مكان المستخدم وهويّة هاتفه، من دون تعريف المستهلكين بذلك».
http://www.ftc.gov/news-events/press-releases/2013/12/android-flashlight-app-developer-settles-ftc-charges-it-deceived.

5. أحيانـاً، تفـرض الرقابة بالإكراه. وكي أحصل على ضمان لسـلعة ما، غالباً ما يفـرض عليّ إعطاء معلومات إلى الشركة التي صنعت تلك السلعة.

6. خلال أيام من البحث على «غوغل» عن مكان لقضاء إجازة، بدأتُ في تلقي إعلانات من «ترافيلوسـتي» عن ذلك المكان. ولا أملك حساباً في موقع «ترافيلوستي».

7. بيتر إكرســلي (21 سبتمبر 2009). «مؤسّســة الحدود الإلكترونيّة». مقال: «كيف تتعرّف الشركات التي تتبعّك على الــويب»، معظم ما تفعله (وكيف تساعدها شركات الــسوشال ميديا» في ذلك)».
Electronic Frontier Foundation,
https://www.eff.org/deeplinks/2009/09/online-trackers-and-social-networks.
8. صاموئيـل غيبـس (28 أكتوبـر 2013). صحيفـة **الغارديان**. مقـال: «أداة «لايـت بيم» من محـرّك البحث «فايرفوكس» تظهر لك من يلاحقك على الإنترنت».
Guardian,
http://www.theguardian.com/technology/2013/oct/28/mozilla-lightbeam-tracking-privacy-cookies
9. 241 آليكـس مادريغـال (29 فبراير 2012). مجلة آتلانتك. مقـال: «أنا ملاحق. كيف عمد «غوغل»- و104 شركات أخرى- إلى ملاحقتي على الإنترنت».
http://www.theatlantic.com/technology/archive/2012/02/im-being-followedhow-google-151-and-104-other-companies-151-are-tracking-me-on-the-web/253758.
10. جوليـا أنغويـن (30 يوليـو 2010). صحيفة **وول ســتريت جورنـال**. «منجم الذهب الجديـد على الإنترنت: أسرارك».
http://online.wsj.com/news/articles/SB100014240527487039409045753950735 12989404
11. آندرو كانينغهام (5 يوليو 2013). موقع «آرس تكنيكا». مقال: «شركة سامســونغ وجاي- زي يعطون درساً متقدّماً في ما لا يجب فعله في التطبيقات الرقمية».
Ars Technica,
http://arstechnica.com/gadgets/2013/07/samsung-and-jay-z-give-the-internet-amasters-class-in-how-not-to-make-an-app.
12. فرانسيس شانغ، فومينغ شييه ودانيال فايتزنر. (4-8 نوفمبر 2013). ورشة عمل عن الخصوصيّة في المجتمع الإلكترونــي، برلين، ألمانيا. ورقة بحث: «لا مفاجآت: قياس مــدى تدخليّة تطبيقات الخلوي بقياس الانحرافات عن السياق».
12th ACM Workshop on Privacy in the Electronic Society (WPES'13), Berlin, Germany,
http://dl.acm.org/citation.cfm?id=2517864
13. دوغلاس راشكوف (6 يوليو 2012). شبكة «سي آن آن». «هل يتجسّس مقدم خدمة الإنترنت عليك»؟
CNN,
http://www.cnn.com/2012/07/06/opinion/rushkoff-online-monitoring.
ديفيـد كرافتـس (5 فبراير 2013). مجلة وايرد. «أصبح مقدّمو خدمة الإنترنت يبحثون الآن عن التعديات على حقوق الملكيّة الفكريّة».
Wired,
http://www.wired.com/2013/02/copyright-scofflaws-beware.
14. كايسي جونستون (3 ديسمبر 2012). «كيف تصبح مُراقِباً من جهاز التلفزيون؟ جرّب وضع كاميرا على جهاز الربط مع الإنترنت».
Ars Technica,
http://arstechnica.com/tech-policy/2012/12/how-to-get-targeted-ads-on-your-tv-a-camera-in-your-settop-box.
كريســتوفر زارا (26 يوليو 2013). «هل يتجسّــس جهــاز الكابل التلفزيوني عليك؟ إنّ نشــطاء الخصوصيّة يخشون أن مايكروسوفت وفاريزون تفعله».
International Business Times,
http://www.ibtimes.com/your-cable-box-spying-you-behaviordetecting-devices-verizon-microsoft-others-worry-privacy-1361587

15. إنـه أمر مثير أننا نسـتخدم أفكاراً آتيـة من عالم الخيال في وصـف مجريات الرقابـة والخصوصيّة، كوصفها بالأورويلية أو الكافكاويّة أو بما وصفه تولكين في رواية عين على سورون. بروس شناير (18 إبريل 2014)، «المجاز في الرقابة». كتاب شناير: عن الأمن.
https://www.schneier.com/blog/archives/2014/04/metaphors_of_su.html.

16. بيتر إكرسلي (يوليو 2010). ورقة بحث: «ما مدى فرادة متصفحك للإنترنت»؟
Proceedings of the 10th International Conference on Privacy Enhancing Technologies,
https://panopticlick.eff.org/browser-uniqueness.pdf.

كيتون ماوري وهوفاف شاتشام (24 مايو 2012). «مكتمل بالبكسيل: بصمات في نسيج «آتش تي أم آل 5»».
Web 2.0 Security and Privacy, San Francisco, California,
http://cseweb.ucsd.edu/~hovav/papers/ms12.html

جوليا أنغوين (21 يوليو 2014). مقال: «تعرّف إلى أداة الملاحقة على الـ«ويب» التي يستحيل صدّها نظرياً». موقع «بروبابليكا».
Pro Publica,
http://www.propublica.org/article/meet-the-online-tracking-device-that-is-virtually-impossible-to-block.

غونيس آكار وآخرون (10 أغسطس 2014). ورقة بحث: «الإنترنت لا تنسى أبداً: إنفلات ميكانيزمات الملاحقة».
ACM Conference on Computer and Communications Security (CCS 2014), Scottsdale, Arizona,
https://securehomes.esat.kuleuven.be/~gacar/persistent/index.html.

17. «غوغل» (5 يوليو 2014). رد على تدوين: إزالة القيود على مستخدمي «غوغل+».
https://plus.google.com/+googleplus/posts/V5XkYQYYJqy.

18. يعيد «فيسبوك» النظر في سياسته تلك، بعد مواجهات مع مستخدمين تضرّروا منها.
Facebook (2014), «What names are allowed on Facebook?»
https://www.facebook.com/help/112146705538576.

رييـد آلبرغوتـي (2 أكتوبر 2014). صحيفة وول سـتريت جورنال. مقال: «فيسـبوك يغيّر سياسـة الاسـم الحقيقي، بعد زوبعة احتجاج من متنكّرين».
Wall Street Journal,
http://online.wsj.com/news/articles/SB100008723963904441658045780087405 78200224.

19. تغـيّر موقـف الناس حيال دفع المال، إلى حدّ ما. إذ يدفع كثيرون منا أموالاً قليلة، أو حتى كثيرة مقسّـطة لزمن طويل، للحصول على تطبيقات للخلوي، لكن منحى الرقابة في الأعمال على الإنترنت لم يتبدّل. وحتى التطبيقات التي تدفع مالاً لقاء الحصول عليها، تتجسّس عليك.

20. سكوت برادنر (3 أغسطس 2010). «نتوورك ورلد». مقال: «ثمن الإنترنت المجاني: قطعة من روحك».
Network World,
http://www.networkworld.com/columnists/2010/080310bradner.html

21. كـورت أوبسـاهل (28 إبريل 2010). «مؤسّسـة الحـدود الإلكترونيّة». «مراجعة: تآكل سياسـة «فيسـبوك» للخصوصيّة».
Electronic Frontier Foundation,
https://www.eff.org/deeplinks/2010/04/facebook-timeline

22. هنـاك رسـم توضيحي تفاعـلي بنوعيّة ممتازة عـن ذلك الموضوع: مـات ماكينون (15 مايـو 2010). مدوّنة إلكترونيّة. «تطوّر الخصوصيّة على «فيسبوك»».
http://mattmckeon.com/facebook-privacy.

23. شـبكة «سي تي في نيوز» عن «وكالة أسوشـيتيد برس». «مراجعة زمنيّة: نظرة إلى التطوّرات المتّصلة بسياسـة «غوغل» بشأن الاهتمامات المتعلّقة بالخصوصيّة».

CTV News,
http://www.ctvnews.ca/sci-tech/timeline-a-look-at-developments-linked-to-google-privacyconcerns-1.1220927.

24. ريتش موغول (25 يونيو 2014). مجلة ماك وورلد. مقال: «لماذا تهتم «آبل» فعلياً بخصوصيّتك»؟

Macworld,
http://www.macworld.com/article/2366921/why-apple-really-cares-about-your-privacy.html

25. تشـارلز آرثـر (18 سـبتمبر 2014). صحيفة الغارديـان. مقال: «تيم كـوك، رئيس «آبـل»، يهاجم «غوغل» و«فيسبوك» بسبب ثغرات في الخصوصيّة».

Guardian,
http://www.theguardian.com/technology/2014/sep/18/apple-tim-cook-google-facebook-privacy-surveillance.

26. جـاي غريني (18 مارس 2014). «شركـة «آمازون» تدخل بيسر تجارة جانبيّة قيمتها بليون دولار: الإعلانات عن التخفيضات».

Union Bulletin,
http://union-bulletin.com/news/2014/mar/18/amazon-easing-1b-sideline-business-ad-sales

ناديـا توما ولورا سمبسـون (23 ينايـر 2014)، مجلة آدفرتايزنغ آيج، «لمـاذا لا يخاف الناس من تخزين البيانات في «آمازون»، بينما يخافونها في «فيسبوك»»؟

Advertising Age,
http://adage.com/article/guest-columnists/americans-scared-amazon-s-data-store/290953

27. آمـي حرمـون (24 أغسـطس 2001). صحيفة نيويـورك تايمس، مقال: «مـع وضع البيانـات العامة على الإنترنت، يعتقد البعض أنها باتت عامة بصورة فائضة».

New York Times,
http://www.nytimes.com/2001/08/24/nyregion/as-public-records-go-online-some-say-they-re-too-public.html

مارك آكرمان (26 أغسطس 2013). مقال: «بيع البيانات العامة إلى المسوّقين يدر أموالاً كثيرة على الحكومات».
CBS Denver,
http://denver.cbslocal.com/2013/08/26/salesof-public-data-to-marketers-can-mean-big-for-governments

28. ثمة مقال جيّد عن «آكزيوم»، ناتاشـا سـنغر، (16 يونيو 2012)، صحيفة نيويورك تايمس، «رسم الخرائط الجينيّة للزبائن وبيعها».

New York Times,
http://www.nytimes.com/2012/06/17/technology/acxiom-the-quiet-giant-of-consumer-database-marketing.html.

29. يقدّر «المنتدى العالمي للخصوصيّة» أنّ هناك قرابة 4 آلاف سمسـار للمعلومات. بام ديكسـون (18 ديسـمبر 2013). «شـهادة بام ديكسـون، المدير التنفيذي لـ«المنتدى العالمي للخصوصيّة» أمام «لجنة التجارة والعلوم والمواصلات»، في مجلس الشـيوخ الأميركي: ما هي المعلومات التي يملكها سـماسرة البيانات عن المسـتهلكين، وكيف يستخدمونها»؟

World Privacy Forum,
http://www.worldprivacyforum.org/2013/12/testimony-what-information-do-data-brokers-have-on-consumers

30. كريغ تيمبرغ (27 مايو 2014). صحيفة واشنطن بوست. مقال: «سماسرة البيانات يستعملون «بلايين» النقاط لرسم بروفايلات عن الأميركيّين».
Washington Post,
http://www.washingtonpost.com/business/technology/brokers-use-billions-of-data-points-to-profile-americans/2014/05/27/b4207b96-e5b2-11e3-a86b-362fd5443d19_story.html.

31. أجرت صحيفة وول ستريت جورنال سلسلة تحقيقات عن الكميات الضخمة من بيانات الرقابة التي تجمعها شركات مختلفة. نشرت تلك التحقيقات تحت اسم مرجعي «ما الذي يعرفونه؟»، وتتوافر على موقع الصحيفة.
Wall Street Journal, «What They Know» series index,
http://online.wsj.com/public/page/whatthey-know-digital-privacy.html.

32. «لجنة التجارة والعلوم والمواصلات»، في مجلس الشيوخ الأميركي، «مكتب الإشراف والمراقبة». طاقم موظّفي الأغلبيّة (18 ديسمبر 2013). «مراجعة بصدد صناعة سماسرة المعلومات: جمع بيانات المستهلكين واستخدامها وبيعها لأغراض تسويقيّة». تقرير الطاقم المقدّم إلى رئيس الأغلبية روكفلر.
http://consumercal.org/wpcontent/uploads/2013/12/senate_2013_data_broker_report.pdf

33. لويس بيكيت (13 سبتمبر 2013). موقع «بروبابليكا»، مقال: «كل ما نعرفه عما يعرفه سماسرة البيانات عنك».
Pro Publica,
https://www.propublica.org/article/everything-we-know-about-what-data-brokers-know-about-you

34. ناتاشا سنغر (5 سبتمبر 2013). صحيفة نيويورك تايمس. مقال: «شركة «أكزيوم» تتيح للمستهلكين رؤية البيانات التي تجمعها».
New York Times,
http://www.nytimes.com/2013/09/05/technology/acxiom-lets-consumers-see-data-it-collects.html

35. 267 تشارلز دوهيغ (20 مايو 2007). صحيفة نيويورك تايمس. مقال: «مخادعة المسنين، مع دعم من الشركات».
New York Times,
http://www.nytimes.com/2007/05/20/business/20tele.html.

36. «لجنة التجارة والعلوم والمواصلات»، في مجلس الشيوخ الأميركي، «مكتب الإشراف والمراقبة». طاقم موظّفي الأغلبيّة (18 ديسمبر 2013). «مراجعة بصدد صناعة سماسرة المعلومات: جمع بيانات المستهلكين واستخدامها وبيعها لأغراض تسويقيّة». تقرير الطاقم المقدّم إلى رئيس الأغلبية روكفلر.
http://consumercal.org/wp-content/uploads/2013/12/senate_2013_data_broker_report.pdf

37. جوزيف تورو (7 فبراير 2012)، مجلة آتلانتيك، مقال: «دليل إرشادي إلى صناعة الإعلام الرقمي التي تتجسّس على كل نقرة تجريها».
Atlantic,
http://www.theatlantic.com/technology/archive/2012/02/a-guide-to-the-digital-advertisingindustry-thats-watching-your-every-click/252667.

38. ليس معروفاً من قال تلك العبارة أولاً. جوناثان زيترين (21 مارس 2012). «المدوّنات الإلكترونيّة لجامعة هارفرد». «قول سارٍ: «إذا كان شيء ما مجانياً، فأنت لست المستهلك بل المنتَج».
The Future of the Internet and How to Stop It,
http://blogs.law.harvard.edu/futureoftheinternet/2012/03/21/meme-patrol-when-something-online-isfree-youre-not-the-customer-youre-the-product

39. نلسون وايات (7 نوفمبر 2013)، صحيفة فانكوفر صن، مقال: «النائب السابق للرئيس الأميركي آل غور، يتوقّع أن يكسب المشرّعون معركة الرقابة».

Vancouver Sun,
http://www.vancouversun.com/news/Former+vicepresident+Gore+predicts+lawmakers+will+rein/9129866/story.html.

40. لورانس غرين (5 يوليو 2010)، صحيفة التلغراف، مقال: «لماذا يعطيك الابتكار نجاحاً أكبر مما يفعله المال».
Telegraph,
http://www.telegraph.co.uk/finance/businessclub/7872084/Why-creativity-will-buy-you-more-success-than-money.html.

41. على الأقل، ذلك ما تقوله النظريّات. هناك من يحاجج بأنّ ذلك ليس بالكفاءة المرجوة. دوغلاس راشكوف (2013). كتاب صدمة الحاضر: عندما يحدث كل شيء الآن.
Present Shock: When Everything Happens Now, Current,
http://www.rushkoff.com/present-shock.

42. «ريل غرين سيستمز» (2014). «المساعدة في القياس: تطبيق شبكي يجمع الصور الجويّة مع أدوات القياس».
https://www.realgreen.com/measurement_assistant.html.

43. ناثان آبز (أكتوبر 2012). «تأثير «البيانات الضخمة» على مآل الحملات السياسيّة: الإعلان السياسي الموجّه إلى مجموعات ميكرويّة في انتخابات الرئاسة للعام 2012».
Interactive Advertising Bureau,
http://www.iab.net/media/file/Innovations_In_Web_Marketing_and_Advertising_delivery.pdf

44. مايكل شيرر (7 نوفمبر 2012)، مجلة تايم، مقال: «العالم الداخلي للمتهمي البيانات الذين ساعدوا في فوز أوباما».
Time,
http://swampland.time.com/2012/11/07/inside-the-secret-world-of-quants-and-data-crunchers-who-helpedobama-win.
ساشا آيزنبرغ (19 ديسمبر 2012). موقع «إم آي تي تكنولوجي ريفيو»، مقال: «كيف استعملت حملة الرئيس أوباما «البيانات الضخمة» في تعبئة الناخب الفرد».
MIT Technology Review,
http://www.technologyreview.com/featuredstory/509026/how-obamas-team-used-big-data-to-rally-voters

45. إد بلنكينغتون وآماندا ميشيل (17 فبراير 2012)، صحيفة الغارديان، «أوباما و«فيسبوك» وقوة الصداقة: البيانات في حملة 2012 الانتخابيّة».
Guardian,
http://www.theguardian.com/world/2012/feb/17/obama-digital-data-machinefacebook-election
تانزينا فيغا (20 فبراير 2012)، صحيفة نيويورك تايمس، «بيانات شبكيّة ساعدت في توجيه الإعلانات في حملة 2012 الانتخابيّة».
New York Times,
http://www.nytimes.com/2012/02/21/us/politics/campaigns-use-microtargeting-to-attract-supporters.html

46. حاضراً، يسمح لك كثيرون من سماسرة المعلومات بتصحيح الأخطاء في بياناتهم. ويساهم كل تصحيح تجريه في تحسين نوعيّة البيانات التي يبيعونها لآخرين. إنّ تصحيحاتك تساعدهم، لكنهم يقدمونها كأنها نوع من الحق الذي اكتسبته الآن.

47. في العام 2014، أرسلت شركة «شاترفلاي» رسائل إلى الناس تهنّئهم بالمواليد الجدد، وارتكبت بعض الأخطاء. وتكفّلت تلك الأخطاء بوصول الأمر إلى الصحافة. كشمير هيل (14 مايو 2014)، مجلة فوربس، مقال: «شركة «شاترفلاي» ترسل تهنئة بـ«القادم الجديد» لأشخاص ليس لديهم أطفال».
Forbes,

http://www.forbes.com/sites/kashmirhill/2014/05/14/shutterfly-congratulates-a-bunch-of-people-without-babies-on-their-new-arrivals.

48. تتوافر دلائل ظرفيّة كثيرة عن كيفيّة إفساد الإعلانات الموجهة خطأً للأمور، لكن معظمها يأتي من كوننا نلاحظ الأخطاء أكثر من التنبّه إلى المسار الرئيس للأمر.

49. جلال محمود، جيفري نيكولاس وكليمانس دروس (7 مارس 2014). «تحديد منازل مستخدمي «تويتر»».
arXiv:1403.2345 [cs.SI],
http://arxiv.org/abs/1403.2345

50. هناك مقال يناقش كفاءة الإعلان بواسطة الإنترنت. دريك طومسون (13 يونيو 2014). مجلة آتلانتيك. مقال: «سؤال خطير: هل هناك أي فعاليّة على الإطلاق للإعلان بواسطة الإنترنت»؟
Atlantic,
http://www.theatlantic.com/business/archive/2014/06/a-dangerous-question-does-internet-advertisingwork-at-all/372704.

51. في 2014، أرسلت شركة «أوفيس ماكس» بريداً ترويجياً موجّهاً إلى «مايك ساايي/ طفلته قضت أثناء حادث سيارة/ أو في تجارة جارية». نجم ذلك البريد عن خطأ في قاعدة البيانات، لكنه يبيّن مدى دقّة المعلومات التي يجمعها سماسرة البيانات. آمي ميرك (23 يناير 2014). صحيفة نيويوركر. مقال: «موت في قاعدة البيانات».
New Yorker,
http://www.newyorker.com/online/blogs/currency/2014/01/ashley-seay-officemax-carcrash-death-in-the-database.html

52. بليز أور وآخرون (2 إبريل 2012). جامعة «كارينغي ميلون». «ذكي، مفيد، مخيف ومريب: انطباعات عن الإعلان الموجه وفق السلوك».
CyLab, Carnegie Mellon University, Pittsburgh, Pennsylvania,
https://www.cylab.cmu.edu/research/techreports/2012/tr_cylab12007.html

53. فارهاد مانجوو (23 أغسطس 2012)، موقع «سلايت». مقال: «الوادي غير الحاذق في إعلانات الإنترنت».
Slate,
http://www.slate.com/articles/technology/technology/2012/08/the_uncanny_valley_of_internet_advertising_why_do_creepy_targeted_ads_follow_me_everywhere_i_go_on_the_web_.html.

سارة واطسون (16 يونيو 2014). مجلة آتلانتيك. «بيانات الشبيه الشبحي و«الوادي غير الحاذق» للشخصنة».
Atlantic,
http://www.theatlantic.com/technology/archive/2014/06/data-doppelgangers-and-the-uncanny-valley-of-personalization/372780.

54. مايك مازنيك (11 مارس 2008). مجلة تيك ديرت. مقال: «أين يرتسم الفاصل بين الإعلان المشخصن وإثارة ريبة الناس؟»
Tech Dirt,
http://www.techdirt.com/articles/20080311/121305499.shtml

55. بليز أور وآخرون (2 إبريل 2012). جامعة «كارينغي ميلون». «ذكي، مفيد، مخيف ومريب: انطباعات عن الإعلان الموجه وفق السلوك».
CyLab, Carnegie Mellon University, Pittsburgh, Pennsylvania,
https://www.cylab.cmu.edu/research/techreports/2012/tr_cylab12007.html

56. إيفان سلينغر (22 أغسطس 2012). موقع «سلايت». مقال: «في أننا نحب أن ندعو التكنولوجيا الجديدة بأنّها «مريبة»».
Slate,
http://www.slate.com/articles/technology/future_tense/2012/08/facial_recognition_software_targeted_advertising_we_love_to_call_new_technologies_creepy_.html

أومير تيني وجولز بولونتسكي (16 سبتمبر 2013). جامعة «يال»، مجلة التكنولوجيا والقانون. مقال: «نظرية المريب: التكنولوجيا والخصوصيّة وتغيّر الأعراف الاجتماعيّة».
Yale Journal of Law & Technology,
http://yjolt.org/theory-creepy-technology-privacyand-shifting-social-norms.

57. سارة م. واتسون (16 سبتمبر 2014). قناة «الجزيرة» وموقعها الإلكتروني. مقال: «اسأل جهاز فك تشفير قنوات التلفزيون: التربص بالضربات».
Al Jazeera,
http://america.aljazeera.com/articles/2014/9/16/the-decoder-stalkedbysocks.html

58. مايك أيزاك (2 نوفمبر 2011). مجلة وايرد. مقال: «سياسة «غوغل» الجديدة في «الشفافيّة» تهدف إلى خفض الشعور بالارتياب».
Wired,
http://www.wired.com/2011/11/google-ad-transparency-target.
تود إيزيك (27 فبراير 2012)، مجلة فوربس، مقال: «ربما توصلك «البيانات الضخمة» إلى الارتياب، لكن الشفافيّة تفيد في درئه».
Forbes,
http://www.forbes.com/sites/toddessig/2012/02/27/big-data-got-you-creeped-out-transparency-can-help

59. تشارلز دوهيغ (19 فبراير 2012). صحيفة نيويورك تايمس. مقال: «كيف تعرف الشركات أسرارك»؟
New York Times,
http://www.nytimes.com/2012/02/19/magazine/shopping-habits.html

60. كشمير هيل (21 أغسطس 2013)، مجلة فوربس، مقال: «صعود ظاهرة استعمال برامج صدّ الإعلانات».
Forbes,
http://www.forbes.com/sites/kashmirhill/2013/08/21/use-of-ad-blocking-is-on-the-rise

61. فكتور ليكرسون (7 مارس 2014). مجلة تايم. مقال: «قيمة الإعلان على «تويتر» في تدنٍّ مطّرد».
Time,
http://time.com/16032/twitter-ad-prices-decline
برايان ووماك (16 إبريل 2014). مقال: «عائدات «غوغل» أقل من التوقّعات، وسقوط مردود الإعلانات».
Bloomberg Business Week,
http://www.businessweek.com/news/2014-04-16/google-revenue-fallsshort-of-estimates-as-ad-prices-decline-1.

62. إميلي ستيل (13 يونيو 2013). صحيفة فايننشال تايمس. مقال: «الشركات تهرع صوب بيانات المستهلك».
Financial Times,
http://link.ft.com/r/S4XZQQ/Z8K8I2/9ZND5E/972MV7/VTD3N8/SN/h
كين فيغيريدو (19 يونيو 2013). مقال: «أسعار بيانات المستهلك وقيمتها».
More with Mobile,
http://www.more-with-mobile.com/2013/06/prices-and-value-ofconsumer-data.html

63. تريستان لويس (13 سبتمبر 2013). مجلة فوربس. مقال: «كم يساوي المستهلك الفرد»؟
http://www.forbes.com/sites/tristanlouis/2013/08/31/how-much-is-a-user-worth

64. تيم هوانغ وآدي كامدار (9 أكتوبر 2013). مقال: «نظرية الذروة في الإعلانات ومستقبل الإنترنت».
Peakads.org,
http://peakads.org/images/Peak_Ads.pdf.
تيم هوانغ (19 مارس 2014). مقال: «مؤسّسة الذروة في الإعلانات».
Knight News Challenge,
https://www.newschallenge.org/challenge/2014/feedbackreview/the-peak-advertising-institute

65. دوك سيرلز (23 مارس 2009). مدوّنة إلكترونيّة على «بلوغز» جامعة هارفرد. مقال: «ما بعد انفجار فقاعة الإعلانات».
Doc Searls Weblog,
http://blogs.law.harvard.edu/doc/2009/03/23/after-the-advertising-bubble-bursts

66. موشيه يودكوفسكي (2005). «كرة الثلج والانهيار الثلجي: كيف يؤدّي تفكيك الأشياء إلى ثورات». دار نشر «بيريت- كويهلر».
http://www.pebbleandavalanche.com

67. مارك غراهام (2008). كتاب الجغرافيات المترابطة للتنمية: الإنترنت ونظريات النمو الاقتصادي. «جيوغرافي كومباس 2/3».
http://www.geospace.co.uk/files/compass.pdf

68. 300 مايك مازنيك (19 يونيو 2013). موقع «تيك ديرت». مقال: «المقولات الجديدة في هوليوود: حراس البوابات مذهلون».
Tech Dirt,
https://www.techdirt.com/articles/20130613/18243923466/hollywoods-new-talking-point-gatekeepersare-awesome.shtml.

69. آلينا م. شيركو وروبرت ج. كوفمان (1998) «مركز البحوث عن نظم إدارة المعلومات». ورقة بحث: «تحليل تحوّلات السوق في ظل اختفاء الوسطاء بتأثير الإنترنت: دراسة حال عن مقدّمي خدمات حجز الطيران بواسطة الإنترنت».
Management Information Systems Research Center,
http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.196.4820&rep=rep1&type=pdf.

70. تيم ويليامز (3 يونيو 2013). شبكة «لينكدن». مقال: «اختفاء الوسطاء في أعمال وكالة الإعلان».
LinkedIn,
http://www.linkedin.com/today/post/article/20130603205503-2042198-the-disintermediation-of-the-agency-business

71. كتاب العصر الرقمي الجديد: إعادة رسم مستقبل الشعوب والأمم والأعمال. دار كنوبف.
http://www.newdigitalage.com.

72. كارل شابيرو وهال فاريان (1998). كتاب قواعد المعلوماتيّة: دليل إرشادي إلى اقتصاد الشبكة. دار «هارفرد بيزنس ريفيو برس».
Harvard Business Review Press,
http://www.inforules.com.

73. موقع «كوم سكور» (21 يونيو 2014). دراسة «كوم سكور تنشر تقييمات شهر يونيو 2014 لسوق عمليات البحث».
https://www.comscore.com/Insights/Market-Rankings/comScore-Releases-June-2014-US-Search-Engine-Rankings

74. مايف دوغان وآرون سميث (30 ديسمبر 2013). «مشروع بيو لبحوث الإنترنت». ورقة: «تحديث معلومات عن الـ«سوشال ميديا»».
Pew Research Internet Project,
http://www.pewinternet.org/2013/12/30/social-media-update-2013

75. تروي (12 مايو 2013). «مقتطفات من الكتاب الأميركي للمراجعة السنويّة عن ميول المستهلك».
AALB.com's Discussion Forum,
http://aalbc.com/tc/index.php/topic/2051-highlights-from-the-us-book-consumer-annual-review

76. تريفــس تيم (24 يوليو 2014)، مجلة فوربس، مقال: «نمو عائدات «كومكاســت» بــ15% بفضل نمو قوي للــ«برودباند»».
Forbes,
http://www.forbes.com/sites/greatspeculations/2014/07/24/comcast-earnings-grow-15-on-good-broadband-growth

77. ماثيــو فــوردال (2 فبراير 2001). شــبكة «إيه بي سي نيــوز». مقال: «موقع «إي باي» يخفــي عناوين البريد الإلكتروني».
ABC News,
http://abcnews.go.com/Technology/story?id=98958

78. موقــع «إي باي» (1 أكتوبر 2011). «عنوان البريد الإلكتروني وبعض الوصلات الإلكترونيّة، لم يعد مســموحاً بهم في القوائم».
http://pages.ebay.com/sellerinformation/news/links2011.html

79. موقع «إي باي» (2 أكتوبر 2012). «إلى الباعة: عناوين البريد الإلكتروني وبعض الوصلات الإلكترونيّة لم يعد مسموحاً بها في التراسل بين مستخدم وآخر».
http://announcements.ebay.com/2012/10/sellers-e-mail-addresses-and-someurls-no-longer-allowed-in-member-to-member-messages

80. ســتيفن ليفــي (22 إبريل 2014). مجلــة وايرد. «جولة في العلــم الذي يوصل تدويناتك المذعــورة- الذكيّة في «فيسبوك» و«تويتر»».
Wired,
http://www.wired.com/2014/04/perfect-facebook-feed

81. نايت أندرســون (24 يوليــو 2008). مقال: «0.6 % لخيار الخروج: «نيبــو آد» يخبّئ وصلة إلكترونيّة ضمن 5000 كلمة عن سياسة الخصوصيّة».
Ars Technica,
http://arstechnica.com/uncategorized/2008/07/06-opt-out-nebuad-hides-link-in-5000-word-privacy-policy

82. بروس شناير (26 نوفمبر 2012)، مجلة وايرد، مقال: «في الأمن، عدنا إلى الإقطاع».
Wired,
http://www.wired.com/2012/11/feudal-security.

83. راشــيل كينــغ (15 أكتوبر 2012). شــبكة «زد نت». مقال: «تقاريــر تؤكّد أن الجمهور يحــب فعليّاً بالتأكيد التخزين في سُحُب المعلوماتيّة».
ZDNet,
http://www.zdnet.com/consumers-actually-really-like-cloud-storage-report-says-7000005784

84. هناك مدخل جيّد لشرح «حوســبة السحاب»: ميتشل آرمبرســت وآخرون (10 فبراير 2009). تقرير تقني من «جامعة كاليفورنيا- بيركلي»: «فوق السحب: وجهة نظر بيركلي في حوسبة السحاب».
Technical Report No. UCB/EECS-2009-28, Electrical Engineering and Computer Sciences, University of California at Berkeley,
http://www.eecs.berkeley.edu/Pubs/TechRpts/2009/EECS-2009-28.pdf.

85. بمبــادرة ذاتيّة منهما، ســلّمت شركتا «غوغل» و«مايكروســوفت» أشــخاصاً مشــتبهاً فيهــم بخصوص جنس الطفولة الإباحي إلى الــ«إف بي آي».
روبرت ماكفرســون (4 أغســطس 2014). موقع «ياهــو نيوز». مقال: «محرّك «غوغــل» يدافع عن مبادرته بصدد جنس الطفولة الإباحي».
Yahoo! News,
http://news.yahoo.com/google-defends-child-porn-tip-offs-police-025343404.html
ليو كيليون (6 أغســطس 2014)، هيئة «بي بي سي». مقال: «أدلة من مايكروســوفت أدّت إلى اعتقالات بصدد جنس الطفولة الإباحي في بنسلفانيا».

BBC News,
http://www.bbc.com/news/technology-28682686.

86. جوناثان زيترين (2009)، فصل: «معدّات مربوطة، وبرامج هي خدمات؛ وتدعيم متكامل»، في كتاب **مستقبل الإنترنت وكيف نوقفه**، «مطبعة جامعة يال».
Yale University Press,
http://dash.harvard.edu/bitstream/handle/1/4455262/Zittrain_Future%20of%20the%20Internet.pdf

87. ميغ آلبوس (5 سبتمبر 2013). مقال: «كي لا ترفضك «آبل»!
PBS Producer Exchange,
https://projects.pbs.org/confluence/pages/viewpage.action?pageId=34046325.

88. براد ستون (18 يوليو 2009). صحيفة **نيويورك تايمس**. مقال: «آمازون تزيل كتب أورويل من «كيندل».
New York Times,
http://www.nytimes.com/2009/07/18/technology/companies/18amazon.html

89. سام غروبارت (14 نوفمبر 2013). مجلة **بيزنس ويك**. مقال: «صُنّاع البرامج ينساقون صوب نموذج الاشتراك».
Business Week,
http://www.businessweek.com/articles/2013-11-14/2014-outlook-software-makers-subscription-drive

90. ديفيد بوغ (17 سبتمبر 2013). مجلة **ساينتيفك أميركان**. مقال: «نموذج الاشتراك في برامج «أدوبي» يعني أنك لن تمتلك برمجياتك أبداً».
Scientific American,
http://www.scientificamerican.com/article/adobe-software-subscription-modelmeans-you-cant-own-your-software.

91. يمارس «غوغل» سياسة أفضل من غيره في مسألة نقل المستخدمين معلوماتهم معهم حينما يتركون خدماته.

92. هنري فاريل (خريف 2013). مجلة **ديموقراطيّة** العدد 30. «النخب الثقافيّة للتقنية».
Democracy 30,
http://www.democracyjournal.org/30/the-tech-intellectuals.php

93. ليس ذلك للقول إنّ تلك الأشياء أساسيّة، وإنّه من المستحيل الاستمرار من دونها. لا أملك حساباً على «فيسبوك». أعرف أشخاصاً لا يملكون هواتف خلوية، وهناك شخص لا يتسوّق بواسطة الإنترنت إطلاقاً. لدينا خيار ما، لكن العيش من دون تلك الأشياء صعب تماماً، على المستويين الشخصي والمهني.

94. جيسيكا غولدشتاين (24 إبريل 2014). مقال: «مقابلة مع امرأة بذلت قصارها كي تخفي حملها عن «البيانات الضخمة»».
Think Progress,
http://thinkprogress.org/culture/2014/04/29/3432050/can-youhide-from-big-data

الفصل 5: الرقابة والسيطرة الحكوميتان

1. بارتون غيلمان وآشكان سلطاني (14 أكتوبر 2013). صحيفة واشنطن بوست. مقال: «تجمع «وكالة الأمن القومي» ملايين دفاتر العناوين في البريد الإلكتروني عالميّاً».

Washington Post,
http://www.washingtonpost.com/world/national-security/nsa-collects-millions-of-email-address-books-globally/2013/10/14/8e58b5be-34f9-11e3-80c6-7e6dd8d22d8f_story.html

بارتون غيلمان وآشكان سلطاني (30 أكتوبر 2013). صحيفة واشنطن بوست. مقال: «وفق وثائق سنودن، تخترق «وكالة الأمن القومي» روابط إلكترونيّة في مراكز بيانات «ياهوو» و«غوغل» عالميّاً».

Washington Post,
http://www.washingtonpost.com/world/national-security/nsa-infiltrates-links-to-yahoo-google-data-centers-worldwide-snowden-documents-say/2013/10/30/e51d661e-4166-11e3-8b74-d89d714ca4dd_story.html

بارتون غيلمان ولورا بواتراس (7 يونيو 2013)، صحيفة واشنطن بوست، مقال: «الاستخبارات البريطانيّة والأميركيّة تنقّب في بيانات من 9 شركات للإنترنت، ضمن برنامج سريّ واسع».

Washington Post,
http://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companiesin-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html.

2. توجيه تنفيذي من مكتب رئيس الولايات المتحدة (24 أكتوبر 1952). مذكّرة إلى وزير الخارجية ووزير الدفاع: «وكالة استخباراتيّة للاتصالات»، «وكالة الأمن القومي للولايات المتحدة».

http://www.nsa.gov/public_info/_files/truman/truman_memo.pdf.

3. توماس بيرنز (1990). كتاب جذور وكالة الأمن القومي 1940-1952، عن «المركز الأميركي لتاريخ التشفير»، «وكالة الأمن القومي».

http://www.nsa.gov/public_info/_files/cryptologic_histories/origins_of_nsa.pdf.

4. كتب علماء سياسة عن الفارق بين الأسرار والألغاز أو بين الألغاز والأحجيات. جوزيف س. ناي جونيور. مجلة فورين آفيرز. عدد (يوليو/أغسطس 1994). مقال: «التطلّع إلى المستقبل».

Foreign Affairs,
http://www.foreignaffairs.com/articles/50102/joseph-s-nye-jr/peering-into-the-future

جيوفري تريفرتون (سبتمبر 2001). بحث: «إعادة هيكلة الاستخبارات القوميّة لتتلاءم مع عصر المعلومات».
Research Brief 5, EuropeanUnion Center for California,
http://eucenter.scrippscollege.edu/files/2011/06/Treverton-05.pdf.

5. دان غير (9 أكتوبر 2013). «مبادلات في الأمن السبراني».

http://geer.tinho.net/geer.uncc.9x13.txt

6. بموجب قانون العام 1978 عن محكمة «فيسا» التي تنظّم رقابة «وكالة الأمن القومي»، يفترض بالأشخاص المستهدفين داخل الولايات المتحدة أن يكونوا «عملاء دولة أجنبيّة». عندما عُدّل ذلك القانون في 2008، بات تعريف الهدف ينطبق على أي أجنبي.

7. دانا بريست (21 يوليو 2013). صحيفة واشنطن بوست. مقال: «تغذى نمو «وكالة الأمن القومي» من الحاجة إلى استهداف إرهابيّين».

Washington Post,
http://www.washingtonpost.com/world/national-security/nsa-growth-fueled-by-need-to-target-terrorists/2013/07/21/24c93cf4-f0b1-11e2-bed3-b9b6fe264871_story.html

8. فعلت الوكالة ذلك في 1984. ويليام ج. برود (8 نوفمبر 1998). صحيفة **نيويورك تايمس**. مقال: «قصّة غواصة تجسّس أميركيّة شُجاعة».

New York Times,

http://www.nytimes.com/1998/11/08/us/a-tale-of-daring-american-submarine-espionage.html

9. موقع «غوغل» (2014). «مواقع مراكز البيانات».

https://www.google.com/about/datacenters/inside/locations/index.html.

10. بارتون غيلمان وغريغ ميلر (29 أغسطس 2013). صحيفة **واشنطن بوست**. مقال: «نجاحات شبكة الجواسيس الأميركيّين وفشلها وأهدافها، تظهر تفصيليّاً في «صندوق أسود» يلخّص ميزانيتها».

Washington Post,

http://www.washingtonpost.com/world/national-security/black-budget-summary-details-us-spy-networks-successes-failures-and-objectives/2013/08/29/7e57bb78-10ab-11e3-8cdd-bcdc09410972_story.html

إيوين ماكآسكيل وجوناثان واتس (29 أغسطس 2013). صحيفة **الغارديان**. مقال: «مصدر سري رفيع يكشف أن إنفاق الاستخبارات الأميركيّة تضاعف منذ 11/9».

Guardian,

http://www.theguardian.com/world/2013/aug/29/us-intelligence-spending-double-9-11-secret-budget

11. ريان سنغل (10 أكتوبر 2007). مجلة **وايرد**، «الاختراق المحظوظ لمصلحة «وكالة الأمن القومي»: كيف تحوّلت أميركا إلى محوّل مفاتيح لمكالمات العالم».

Wired,

https://web.archive.org/web/20071019223411/http://www.wired.com/politics/security/news/2007/10/domestic_taps

كريستوفر ميمز (8 يونيو 2013). «لماذا تملك «وكالة الأمن القومي» نفاذاً إلى 80 % من المكالمات الشبكيّة حتى من دون «الأبواب الخلفيّة» في محرّك «غوغل»».

Quartz,

http://qz.com/92369/why-nsa-has-access-to-80-of-online-communication-even-if-googledoesnt-have-a-back-door.

12. إيوين ماكآسكل وجيمس بول (2 نوفمبر 2013). صحيفة **الغارديان**. مقال: «بورتريه عن «وكالة الأمن القومي»: لا هدف أصغر من أن يلاحظ، للتوصّل إلى الرقابة الشاملة».

Guardian,

http://www.theguardian.com/world/2013/nov/02/nsa-portrait-total-surveillance.

غلين غرينوالد (2014). كتاب **لا مكان للاختباء: إدوارد سنودن ووكالة الأمن القومي وحال الرقابة في الولايات المتحدة**. (دار ماكميليان للنشر).

http://leaksource.info/2014/07/31/glenn-greenwalds-no-place-to-hide-nsa-documents-excerpts

13. بالطبع لا أعرف ذلك بصورة مؤكّدة. وأورد بيل بليني، وهو مطلّق صافرة إنذار آخر [كحال سنودن]، أن الوكالة تفعل ذلك، لكنه لم يقدّم دليلًا على ذلك. أنطوني لويفنشتاين (10 يوليو 2014)، صحيفة **الغارديان**، مقال: «المقال النهائي لـ «وكالة الأمن القومي» هو السيطرة على الناس كلّهم».

Guardian,

http://www.theguardian.com/commentisfree/2014/jul/11/the-ultimate-goal-of-thensa-is-total-population-control

14. ريان ديفيريه، غلين غرينوالد ولورا بواتراس (19 مايو 2014)، موقع «إنترسبت». مقال: «قراصنة البيانات في الكاريبي: «وكالة الأمن القومي» تسجّل المكالمات الخلوية كافة في الـ«باهاماس».

Intercept,

https://firstlook.org/theintercept/article/2014/05/19/data-pirates-caribbean-nsa-recording-every-cell-phone-call-bahamas

جوليان آسانج (23 مايو 2014)، «إعلان من «ويكيليكس» بصدد تسجيلات الهاتف الجماعيّة للأفغان، من قِبَل «وكالة الأمن القومي».

WikiLeaks,
https://wikileaks.org/WikiLeaks-statement-on-the-mass.html.

15. بارتون غيلمان وغريغ ميلر (29 أغسطس 2013). صحيفة واشنطن بوست. مقال: «نجاحات شبكة الجواسيس الأميركيّين وفشلها وأهدافها، تظهر تفصيليّاً في «صندوق أسود» يلخّص ميزانيتها».
Washington Post,
http://www.washingtonpost.com/world/national-security/black-budget-summary-details-us-spy-networks-successes-failures-and-objectives/2013/08/29/7e57bb78-10ab-11e3-8cdd-bcdc09410972_story.html

16. دانا بريست (21 يوليو 2013)، واشنطن بوست، مقال: «تغذّى نمو «وكالة الأمن القومي» من الحاجة لاستهداف إرهابيّين».
Washington Post,
http://www.washingtonpost.com/world/national-security/nsagrowth-fueled-by-need-to-target-terrorists/2013/07/21/24c93cf4-f0b1-11e2-bed3-b9b6fe264871_story.html.

17. تذهب 70 % من ميزانية الاستخبارات إلى الشركات الخاصة، ويملك 483 ألف متعاقد تفويضات عالية السريّة، ويمثّلون 34 % من أصل 1.4 مليون شخص لديهم تفويضات على ذلك المستوى. روبرت أوهارو جونيور، دانا بريست ومارجواري سنسر (10 يونيو 2013). صحيفة واشنطن بوست. «تسريبات «وكالة الأمن القومي» تظهر مدى اعتماد المؤسّسة الاستخباراتيّة على متعاقدين خارجيّين».
Washington Post,
http://www.washingtonpost.com/business/nsa-leaks-put-focus-onintelligence-apparatuss-reliance-on-outside-contractors/2013/06/10/e940c4ba-d20e-11e2-9f1a-1a7cdee20287_story.html.
Jonathan Fahey and Adam Goldman (10 Jun 2013),
«Leak highlights key role of private contractors,» Associated Press,
http://bigstory.ap.org/article/leak-highlights-key-role-private-contractors

18. بارتون غيلمان وغريغ ميلر (29 أغسطس 2013). صحيفة واشنطن بوست. مقال: «نجاحات شبكة الجواسيس الأميركيّين وفشلها وأهدافها، تظهر تفصيليّاً في «صندوق أسود» يلخّص ميزانيتها».
Washington Post,
http://www.washingtonpost.com/world/national-security/black-budget-summary-details-us-spy-networks-successes-failures-and-objectives/2013/08/29/7e57bb78-10ab-11e3-8cdd-bcdc09410972_story.html

19. ستيفن آفترغود (مارس 2014). بحث: «بيانات ميزانية الاستخبارات». «رابطة العلماء الأميركيّين- برنامج موارد الاستخبارات».
Federation of American Scientists Intelligence Resource Program,
http://fas.org/irp/budget/index.html

20. «نعتقد أن المهمّات العسكريّة في العراق وأفغانستان تركت آثاراً يصعب قياسها لكنها ضخمة تماماً، في القرارات بشأن تقنيات جمع المعلومات وتقنيّات الاتصالات». ريتشارد كلارك وآخرون (12 ديسمبر 2013)، «الحريّة والأمن في عالم متغيّر: تقرير وتوصيات «لجنة الرئاسة للمراجعة بشأن الاستخبارات وتقنيات الاتصالات»»، المكتب التنفيذي للرئيس الأميركي، ص 187.
http://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf.

21. يُسمّيه المحقّقون الفيدراليّون «12 ثلاث ثلاثات». المكتب التنفيذي للرئيس الأميركي (4 ديسمبر 1981)، «الأمر التنفيذي رقم 12333 - بشأن نشاطات الاستخبارات الأميركيّة». السجل الفيدرالي.

Federal Register,
http://www.archives.gov/federal-register/codification/executive-order/12333.html

أليكس آبدو (29 سبتمبر 2014). «وثائق جديدة تلقي الضوء على أقوى أدوات «وكالة الأمن القومي»».

Free Future,
https://www.aclu.org/blog/national-security/new-documents-shed-light-one-nsas-most-powerful-tools

22. مارك جايكوكس (5 نوفمبر 2013). مؤسّسة الحدود الإلكترونيّة. مقال: «3 تسريبات، 3 أسابيع وما الذي عرفناه عن السلطة التجسّسيّة الأخرى للحكومة الأميركيّة: الأمر التنفيذي 12333».

Electronic Frontier Foundation,
https://www.eff.org/deeplinks/2013/10/three-leaks-three-weeks-and-what-weve-learned-about-governments-other-spying

23. الكونغرس الأميركي (2001). «الفصل 215 من التشريع الأميركي «باتريوت آكت»».

http://www.gpo.gov/fdsys/pkg/BILLS-107hr3162enr/pdf/BILLS-107hr3162enr.pdf

24. 350 مارسي ويلر (14 أغسطس 2014). موقع «صالون». مقال: «الأبطال المزيّفون لجورج دبليو بوش: القصة الحقيقيّة للخداع السري في واشنطن».

Salon,
http://www.salon.com/2014/08/14/george_w_bushs_false_heroes_the_real_story_of_a_secret_washington_sham

25. هناك أيضاً «قانون حماية أميركا» للعام 2007. وجرى تجاوزه وإبداله بـ«التعديلات على قانون رقابة الاستخبارات الأجنبيّة»، مع الاحتفاظ بمرجعية التخويلات التي يقدّمها «قانون حماية أميركا». لا نعلم عدد تلك التخويلات، ولا مدى أهميّتها أيضاً. جيمس ريزين (6 أغسطس 2007). صحيفة **نيويورك تايمس**. مقال: «بوش يوقّع قانوناً بتوسيع مدى التنصّت».

New York Times,
http://www.nytimes.com/2007/08/06/washington/06nsa.html

رايان سنغل (6 أغسطس 2007). مجلة وايرد. مقال: «تحليل: قانون جديد يمنح الحكومة 6 شهور كي تحوّل الإنترنت ونُظُم الهاتف، بنية دائمة للتجسّس».

Wired,
http://www.wired.com/2007/08/analysis-new-la.

26. تناقش إحدى وثائق سنودن إجراءات تقليصيّة للوكالة. «وكالة الأمن القومي» (8 يونيو 2007). «إجراءات تقليصيّة استخدمتها الوكالة في ما خصّ مصادرة معلومات ترجع لاستخبارات أجنبيّة، بالتوافق مع الفصل 702 من «قانون رقابة الاستخبارات الأجنبيّة» معدّلاً». موقع صحيفة **الغارديان**.

http://www.theguardian.com/world/interactive/2013/jun/20/exhibit-b-nsa-procedures-document

27. جينفير غرانيك (25 أغسطس 2014)، موقع «جاست سيكيوريتي»، مقال: «الإبلاغ عن اعتراض الاتصالات يطرح سؤالاً أوسع بخصوص تقليص الـ«بيانات الوصفيّة».

Jennifer Granick (25 Aug 2014), «Intercept reporting raises broader metadata minimization question,»
Just Security,
http://justsecurity.org/14327/intercept-reporting-raises-broader-metadata-minimization-question.

Marcy Wheeler (26 Aug 2014), «SPCMA and ICREACH,» *Empty Wheel,*
http://www.emptywheel.net/2014/08/26/spcma-and-icreach

28. بارتون غيلمان، جوليا تاييت وآشكان سلطاني (5 يوليو 2014)، صحيفة واشنطن بوست، مقال: «في بيانات اعتراض الاتصالات، تفوق أعداد غير المستهدفين بما لا يقاس أولئك المصنفين أهدافاً».
Washington Post,
http://www.washingtonpost.com/world/national-security/in-nsaintercepted-data-those-not-targeted-far-outnumber-the-foreigners-who-are/2014/07/05/8139adf8-045a-11e4-8572-4b1b969b6322_story.html

29. نادية كيّالي (21 مايو 2014). موقع «غيزمودو». مقال: «كيف تغيّر «وكالة الأمن القومي» إنفاذ القانون».
Gizmodo,
http://gizmodo.com/how-the-nsa-istransforming-law-enforcement-1579438984

30. رايـان غالاهار (25 أغسـطس 2014). موقع «إنترسـبت». مقال: «محرّك الرقابة: كيـف صنعت «وكالة الأمن القومي» محرك بحثها السري المشابه لـ«غوغل»».
Intercept,
https://firstlook.org/theintercept/2014/08/25/icreach-nsa-cia-secret-google-crisscross-proton

31. حدث التوسّع الأكثر دلالة في سلطات «وكالة الأمن القومي» في العام 2005، تحت مظلّة «قانون تحسين «قانون باتريوت» وإعادة هيكلة تخويلاته». ونُظِر إلى بعض مواد ذلك القانون باعتبارها غير شرعيّة.

32. جون فيلاسنور (30 ديسمبر 2013). مجلة آتلانتك. مقال: «ماذا تعرف عن «مبدأ الطرف الثالث؟»
Atlantic,
http://www.theatlantic.com/technology/archive/2013/12/what-you-need-to-know-about-thethird-party-doctrine/282721.

33. يختصر مصطلح «آي أم سي آي» عبارة «الهويّة العالميّة للمشترك في الهاتف النقّال» (*International Mobile Subscriber Identity*). وتتمثّل في رقم متسلسل متفرّد يعطى لهاتفك لتمكينه من البث، فيعرف نظام شبكة الخلوي مكان وجودك.

34. الاسـم الشـيفري الآخر هو «آمبرجاك» (*AmberJack*). حاضراً، يسـتعمل «سـتنغراي» بوصفه اسـم النوع لأدوات «آي أم أس آي- كاتشر».

35. جويل هروسـكا (14 يونيو 2014). مجلة إكستريم تيك. ««ستنغراي»: برج زائف للخلوي تستعمله الشرطة وشركات النقل لتتبّعك في الأمكنة كافة».
Extreme Tech,
http://www.extremetech.com/mobile/184597-stingray-the-fake-cell-phone-towercops-and-providers-use-to-track-your-every-move.

36. لورين وولكر (23 سـبتمبر 2014). مجلة نيوزويك. مقال: «وثائق جديدة تكشف معلومات عن أدوات تعقّب تستخدمها الشرطة».
Newsweek,
http://www.newsweek.com/new-documents-reveal-information-about-police-cell-phone-trackingdevices-272746

37. كيم زيتر (19 يونيو 2014). مجلة وايرد. مقال: «رسائل بريد إلكتروني تكشف أن الضبّاط الفيدراليين طلبوا من شرطة فلوريدا خداع القضاة».
Wired,
http://www.wired.com/2014/06/feds-told-cops-todeceive-courts-about-stingray

38. ناثـان فريد ويسـلر (3 يونيـو 2014). مجلة فري فيوتشر عـلى موقع «الاتحاد الأميركـي للحريّات المدنيّة». «جنرالات أميركا الفيدراليون صادروا وثائق مكالمات هاتفيّة من بوليس محلي في محاولة استثنائيّة لمنع وصولها إلى الجمهور».
Free Future,
https://www.aclu.org/blog/national-security-technology-and-liberty/us-marshals-seize-local-cops-cell-phone-tracking-files.

Kim Zetter (3 Jun 2014), «U.S. Marshals seize cops' spying records to keep them from the ACLU,» *Wired*,
http://www.wired.com/2014/06/feds-seize-stingray-documents

39. «المركز القومي لمكافحة الإرهاب» (2007). «مخزن بيانات هويّات الإرهابيّين وبيئتهم [«تايد»] (*TIDE*)».
https://web.archive.org/web/20140712154829/http://www.nctc.gov/docs/Tide_Fact_Sheet.pdf

ريتشارد أ. بست جونيور (19 ديسمبر 2011)، «خدمة بحوث الكونغرس»، مقال: ««المركز القومي لمكافحة الإرهاب»: المسؤوليات والقلق المحتمل للكونغرس».
Congressional Research Service,
http://fas.org/sgp/crs/intel/R41022.pdf

مات سليدج (16 فبراير 2013). صحيفة هافنغتون بوست. مقال: «وثيقة عن بيانات الإرهابيّين في «المركز القومي لمكافحة الإرهاب»».
Huff-ington Post,
http://www.huffingtonpost.com/2013/02/15/national-counterterrorism-center-nctc-terrorist-information_n_2697190.html

40. كارين دي يونغ (25 مارس 2007). صحيفة واشنطن بوست. «قاعدة بيانات الإرهابيّين زادت بأربعة أضعاف في أربع سنوات».
Washington Post,
http://www.washingtonpost.com/wp-dyn/content/article/2007/03/24/AR2007032400944.html.

41. جوليا أنغوين (13 ديسمبر 2013). صحيفة وول ستريت جورنال. مقال: «وكالة أميركيّة لمكافحة الإرهاب تمارس التنصّت بواسطة قاعدة بيانات واسعة لمواطنين».
Wall Street Journal,
http://online.wsj.com/news/articles/SB10001424127887324478304578171623040640006

42. جيرمي سكاهيل وريان دينيرفو (5 أغسطس 2014). موقع «انترسيبت». مقال: «قائد التجسّس: النظام باراك أوباما السري لتتبّع الإرهابيّين بالأرقام».
Intercept,
https://firstlook.org/theintercept/article/2014/08/05/watch-commander

43. إريك شميدت ومايكل شميدت (24 إبريل 2013). صحيفة نيويورك تايمس. مقال: «اسم مفجّر «ماراثون بوسطن» كان على قوائم وكالتين أميركيّتين».
New York Times,
http://www.nytimes.com/2013/04/25/us/tamerlan-tsarnaev-bomb-suspect-wason-watch-lists.html.

44. وزارة العدل الأميركيّة (2014). «فرق العمل لدعم مكافحة الجريمة المنظّمة».
http://www.justice.gov/criminal/taskforces/ocdetf.html.

45. «المكتب التنفيذي للرئاسة الأميركيّة» (2009). «المبادرة القوميّة الشاملة لأمن الفضاء السبراني».
http://www.whitehouse.gov/issues/foreign-policy/cybersecurity/national-initiative

46. روبرت بوكهوسين (5 إبريل 2013). مجلة وايرد. مقال: «يسعى «مكتب الكحول والتبغ والأسلحة الناريّة» إلى صنع قاعدة بيانات «مكثّفة» كي يعرف من هم أصدقاؤك».
Wired,
http://www.wired.com/2013/04/atf-database.

47. ليزا مايرز، دوغلاس باسترناك وريتش غارديلا (14 ديسمبر 2005). شبكة «آن بي سي نيوز». مقال: «هل يتجسّس البنتاغون على الأميركيّين؟»
NBC News,

http://www.nbcnews.com/id/10454316/ns/nbc_nightly_news_with_brian_williams-nbc_news_investigates/t/pentagon-spying-americans

مارسي ويلر (24 يوليو 2007). مقال: «كانينغهام، «سي آي أف إيه» وتشيني: رواية جديدة للتاريخ».
Empty Wheel,
http://www.emptywheel.net/2007/07/24/cunningham-cifa-and-cheney-a-new-chronology

48. في العام 2014، قرّرت محكمة فيدراليّة أنّ تلك الممارسة ليست قانونيّة، وألغت إدانة بممارسة جنس أطفال إباحي، كانت مستندة إلى أدلة المكتب. فيكتوريا كافالير (18 سبتمبر 2014). وكالة «رويترز». مقال: «محكمة أميركيّة تخطّئ ممارسة البحرية رقابة على الحواسيب في سياق تحقيق عن جنس أطفال إباحي».
Reuters,
http://www.reuters.com/article/idUSKBN0HD2EU20140918

49. روبرت مولر (15 نوفمبر 2004). موقع «إف بي آي». «الـ«إف بي آي»: تحسين الاستخبارات من أجل أميركا أكثر أمناً». خطاب في قاعة البلدية في مدينة «لوس أنجلوس».
http://www.fbi.gov/news/speeches/the-fbi-improving-intelligence-for-a-safer-america

«وزارة الأمن الوطني» (4 سبتمبر 2012). «منشورات عن مراكز الانصهار».
http://www.dhs.gov/sites/default/files/publications/Fusion%20Centers%20Handout.pdf

مجلس النواب الأميركي (يوليو 2013). «تقرير موظفي الأغلبيّة عن شبكة وطنية لمراكز الانصهار»، لجنة «وزارة الأمن الوطني».
http://homeland.house.gov/sites/homeland.house.gov/files/documents/CHS%20SLFC%20Report%202013%20FINAL.pdf

50. تورين مناهان (2010). مجلة سوشال جستس. بحث: «مستقبل الأمن؟ عمليات الرقابة في مراكز الانصهار التابعة لوزارة الأمن الوطني».
Social Justice 37,
http://www.socialjusticejournal.org/archive/120_37_2-3/120_07Monahan.pdf.

51. بريسيلا م. ريغان، تورين موناهان وكريستا كرافن (3 ديسمبر 2013). «تركيب المشتبه فيه: إنتاج البيانات وتداولها وتفسيرها في «مراكز الانصهار» لوزارة الأمن الوطني».
Administration and Society,
http://aas.sagepub.com/content/early/2013/11/29/0095399713513141.abstract

52. ميتشل غيرمان وغاي ستانلي (ديسمبر 2013). «الاتحاد الأميركي للحريّات المدنيّة». «ما خطب مراكز الانصهار؟»
American Civil Liberties Union,
https://www.aclu.org/files/pdfs/privacy/fusioncenter_20071212.pdf.

شارون برادفورد فرانكلين وآخرون (6 سبتمبر 2012)، مؤسّسة «مشروع الدستور». مقال: «توصيات إلى مراكز الانصهار: حماية الخصوصيّة والحريّات المدنيّة في سياق الحماية من الجريمة والإرهاب».
Constitution Project,
http://www.constitutionproject.org/pdf/fusioncenterreport.pdf

53. كولن مونيهان (22 آيار 2014). صحيفة نيويورك تايمس. مقال: «رسميّون نشروا شبكة واسعة لمراقبة حركة «احتلوا وول ستريت»».
New York Times,
http://www.nytimes.com/2014/05/23/us/officials-cast-wide-net-in-monitoring-occupy-protests.html

مارا فيرهايدن هيلر وكارل ميسنيو (5 آيار 2014). مؤسّسة «الشراكة لأجل عدالة مدنيّة». مقال: «خروجاً من الظلال: الدور الخفي لـ«مراكز الانصهار» في رقابة على «حركة احتلّوا وول ستريت» والاحتجاج السلمي في الولايات الولايات المتحدة».

Partnership for Civil Justice,
http://www.justiceonline.org/one-nation-under-surveillance/out-of-the-shadowspcjf-report.pdf.

54. «الاتحـاد الأميركـي للحريات المدنيّة» (سـبتمبر 2013). «منفلت وغير موثوق: لا رقابة على إسـاءة اسـتعمال الـ«إف بي آي» السلطة».
https://www.aclu.org/sites/default/files/assets/unleashed-and-unaccountable-fbi-report.pdf.

روبرتو سـكاليز (10 إبريل 2014). صحيفة بوسـطن غلـوب. مقال: «الاتحاد الأميركـي للحريّات المدنيّة» يقاضي الـ«إف بي آي»، أمام المدعي العام لـ«توداشيف»، وفق وثائق فرقة المهمة».
Boston Globe,
http://www.boston.com/news/local/massachusetts/2014/04/10/aclu-sues-fbi-attorney-for-todashev-task-force-records/MYWzetg75Zy3DIpLB1nyrO/story.html

55. «الاتحـاد الأميركـي للحريّـات المدنيّة» (24 أغسـطس 2010). مقال: «وفـق وثيقة جديدة: «الفرق المشـتركة لمكافحة الإرهاب» التابعة للـ«إف بي آي» استهدفت نشطاء مسالمين بالمضايقة والمراقبة السياسيّة».
http://aclu-co.org/new-documents-confirm-fbis-joint-terrorism-task-force-targets-peaceful-activists-for-harassment-political-surveillance

كيفن كوزسـتيلا (4 يوليو 2014)، موقع «ديسنتر»، مقال: «تقارير عن مراجعة من «الفرق المشتركة لمكافحة الإرهاب» التابعة للـ«إف بي آي» وضبّاط فيدراليين كبار، قضية تتعلّق بنشطاء سياسيّين عمرها 30 سنة».
Dissenter,
http://dissenter.firedoglake.com/2014/07/04/fbi-jttf-us-marshalsservice-are-reportedly-visiting-political-activists-about-thirty-year-old-case

56. سـبنسر إكرمان (23 سـبتمبر 2011). مجلة وايرد، مقال: «دليل جديد على تفكير معاد للإسلام، يثير تحدّيات عميقة حيال وعد الـ«إف بي آي» بالإصلاح».
Wired,
http://www.wired.com/2011/09/fbi-islam-domination/all

57. 383 آدم غابات (1 أغسـطس 2013). صحيفة الغارديان، مقـال: «تفتيش منزل امرأة في نيويورك بعد أن بحثت في الإنترنت عن معلومات تتعلّق بطناجر الضغط».
Guardian,
http://www.theguardian.com/world/2013/aug/01/new-york-police-terrorism-pressure-cooker.

كارلـوس ميللر (23 مايو 2014)، مقال: «بوليس من فرقة مكافحة الإرهاب يفتش منزل مصوّر التقط صوراً لمباني الشرطة ».
Photography Is Not a Crime,
http://photographyisnotacrime.com/2014/05/23/terrorist-task-force-cop-visits-man-home-photographing-police-buildings.

سـتيف أنير (11 يوليو 2014)، مجلة بوسطن مغازين، «رفع قضية من «الاتحاد الأميركي للحريّات المدنيّة» ضد الشرطة، بعد فرضه رقابة على مصوّر بسبب «سلوك مريب»».
Boston Magazine,
http://www.bostonmagazine.com/news/blog/2014/07/11/aclu-james-prigoff-terrorism-task-force-lawsuit

58. دنكان كامبل (3 يونيو 2014). مقال: «الكشـف عن مركز سريّ جداً للتنصّت على الإنترنت في الشرق الأوسـط تابع لـ«القيادة الحكوميّة للاتّصالات»».
Register,
http://www.theregister.co.uk/2014/06/03/revealed_beyond_top_secret_british_intelligence_middleeast_internet_spy_base.

59. نيكي هاغر وستيفانيا موريزي (5 نوفمبر 2013). صحيفة لي سبريسو. مقال: «قبرص مقر أميركي/ بريطاني مشترك للتجسّس على الإنترنت في الشرق الأوسط».
L'Espresso,
http://espresso.repubblica.it/inchieste/2013/11/04/news/the-history-of-british-intelligence-operations-in-cyprus-1.139978.
ريتشارد نورتون تايلور (28 نوفمبر 2013). صحيفة الغارديان. مقال: «مذكّرات سريّة تظهر جهود جهازي «إم آي 5» و«إم آي 6» و«القيادة الحكوميّة للاتّصالات» للحفاظ على قبرص قاعدة لهم».
Guardian,
http://www.theguardian.com/uk-news/2013/nov/29/intelligence-mi5-mi6-gchq-cyprusnational-archives
60. سفن بيكر وآخرون (18 يونيو 2014). صحيفة دير شبيغيل، مقال: «كشوفات جديدة عن «وكالة الأمن القومي»: دواخل ملف ألمانيا».
Der Spiegel,
http://www.spiegel.de/international/germany/newsnowden-revelations-on-nsa-spying-in-germany-a-975441.html
هوبرت جود وآخرون (18 يونيو 2014). صحيفة دير شبيغيل، مقال: «التجسّس معاً: التعاون العميق بين ألمانيا و«وكالة الأمن القومي»».
Der Spiegel,
http://www.spiegel.de/international/germany/the-german-bnd-and-americannsa-cooperate-more-closely-than-thought-a-975445.html.
61. جاك فلورو وغلين غرينولد (21 أكتوبر 2013)، صحيفة لوموند، «فرنسا في مقعد مشترك مع «وكالة الأمن القومي»: رقابة شبكات الهواتف».
Le Monde,
http://www.lemonde.fr/technologies/article/2013/10/21/france-in-the-nsa-s-crosshair-phone-networks-under-surveillance_3499741_651865.html.
جاك فلورو وفرانك جوهانس (4 يوليو 2013)، مجلة سوسيتيه، مقال: «كشوفات عن «الأخ الكبير» الفرنسي».
Société,
http://www.lemonde.fr/societe/article/2013/07/04/revelations-on-the-french-big-brother_3442665_3224.html
62. رايان غالاهار (18 يوليو 2014). موقع «إنترسبت». مقال: «كيف وسّع الشركاء السريّون شبكة الصيد لـ«وكالة الأمن القومي»».
Intercept,
https://firstlook.org/theintercept/article/2014/06/18/nsa-surveillance-secret-cable-partners-revealed-rampart-a.
63. جاسون أوم (30 أكتوبر 2013). شبكة «إيه بي سي نيوز- أستراليا». مقال: «خبير في التجسّس يشرح كيف عملت أستراليا «قاعدة تنصّت» لوكالات الاستخبارات الأميركيّة، وضمنها «وكالة الأمن القومي»».
ABC News Australia,
http://www.abc.net.au/news/2013-10-30/australia-acting-as-listening-post-for-us-spy-agencies/5056534
64. غلين غرينولد وريان غالاهار، موقع «إنترسبت»، مقال: «نيوزلندا أطلقت مشروعاً للرقابة العامة فيما أنكرته علانية».
Intercept,
https://firstlook.org/theintercept/2014/09/15/new-zealand-gcsb-speargun-mass-surveillance
65. كريغ تيمبرغ (6 يونيو 2014). صحيفة واشنطن بوست، مقال: «شركة «فودافون» تصرّح بأن الحكومات تجمع معلومات عن مواطنيها، من دون قيود».

Washington Post,
http://www.washingtonpost.com/business/technology/governments-collecting-personal-data-without-limit-says-vodafone/2014/06/06/ff0cfc1a-edb4-11e3-9b2d-114aded544be_story.html

66. مايكل آر. غوردن. (7 فبراير 2014). صحيفة نيويورك تايمس، مقال: «أندونيسيا تتهم أستراليا بالتنصّت على المحادثات».

New York Times,
http://www.nytimes.com/2014/02/18/world/asia/indonesia-takes-aim-at-australia-over-spying-but-not-the-us.html.

67. 393 أندريه سولداتوف وإيرينا بوروغان (خريف 2013). مجلة ورلد بوليسي جورنال. بحث: «حال الرقابة في روسيا».

World Policy Journal,
http://www.worldpolicy.org/journal/fall2013/Russia-surveillance

جيمس أ. لويس (18 إبريل 2014). «مركز الدراسات الاستراتيجيّة العالميّة». بحث: «ملاحظة مرجعيّة عن رقابة الاتصالات في روسيا».

Center for Strategic and International Studies,
http://csis.org/publication/reference-note-russian-communicationssurveillance.

68. تسمى النسخة الأكثر حداثة من ذلك النظام «سورم 3»، وتجمع بيانات رقابة بالجملة عن كل نُظُم الاتّصالات، مع امتلاك نفاذ إلى المعلومات الجارية والتاريخيّة معاً. أندريه سولداتوف وإيرينا بوروغان (21 ديسمبر 2012). مجلة وايرد. مقال: «في الجمهوريات السوفياتيّة السابقة، ما زال الجاسوس التقني يراقبك».

Wired,
http://www.wired.com/2012/12/russias-hand/all.

69. 395 أوين ماثيوز (12 فبراير 2014)، مجلة نيوزويك، مقال: «روسيا تختبر نظاماً لـ«الرقابة الشاملة» في دورة «سوتشي»».

Newsweek,
http://www.newsweek.com/2014/02/14/russia-tests-total-surveillance-sochi-olympics-245494.html

جوشوا كوبشتاين (13 فبراير 2014). صحيفة نيويوركر. مقال: «الإرث الآخر لدورة «سوتشي»».

New Yorker,
http://www.newyorker.com/tech/elements/sochis-other-legacy.

70. غوس هوزين (2010). «منظمة الخصوصيّة الدوليّة». بحث: «الخصوصيّة بوصفها حقاً سياسيّاً».

Index on Censorship 39,
https://www.privacyinternational.org/reports/privacy-asa-political-right/surveillance-of-political-movements#footnote5_5pc3hb7.

71. جيمس أ. لويس (2006). «مركز الدراسات الاستراتيجيّة العالميّة». بحث «هندسة السيطرة: الرقابة على الإنترنت في الصين».

Center for Strategic and International Studies,
http://csis.org/files/media/csis/pubs/0706_cn_surveillance_and_information_technology.pdf

72. صحيفة أستراليان (4 مارس 2011). مقال: «نقد نظام تتبع الهواتف في الصين بوصفه «رقابة الأخ الكبير»».

Australian,
http://www.theaustralian.com.au/news/world/china-mobile-phone-tracking-systemattacked-as-big-brother-surveillance/story-e6frg6so-1226015917086

73. فرانك لانغفيت (29 يناير 2013). مقال: «في الصين، كن حذراً: ربما هنالك كاميرا تراقبك».

NPR Morning Edition,
http://www.npr.org/2013/01/29/170469038/in-china-beware-a-camera-may-be-watching-you

74. كالـوم ماكلويـد (3 ينايـر 2013). صحيفة يو إس داي تـودي، مقال: «رقابة الصين تسـتهدف الجريمة... والمنشقين».
USA Today,
http://www.usatoday.com/story/news/world/2013/01/03/china-security/1802177

75. فيرنـون سـيلفر (8 مارس 2013). مجلة بلومبرغ بيزنس ويك. مقـال: «اختراق نظام الرقابة الصيني على «سكايب»».
Bloomberg Business Week,
http://www.businessweek.com/articles/2013-03-08/skypes-been-hijacked-in-china-and-microsoft-is-o-dot-k-dot-with-it

76. جون ماركوف (1 أكتوبر 2008). صحيفة نيويورك تايمس. مقال: «هناك رقابة على برنامج «سـكايب» في الصين».
New York Times,
http://www.nytimes.com/2008/10/02/technology/internet/02skype.html

77. جـون روبـيرو (13 يناير 2011). مقـال: «شركـة «آر. إي. أم» [صانعة هواتف «بلاك بيري»] تسـمح للهند بالوصول إلى رسائل مستخدمي «بلاك بيري»».
John Ribeiro (13 Jan 2011), «RIM allows India access to consumer BlackBerry messaging,» *CIO,*
http://www.cio.com/article/654438/RIM_Allows_India_Access_to_Consumer_BlackBerry_Messaging.
آمول شـارما (28 أكتوبر 2011). صحيفة وول سـتريت جورنال. مقال: «شركة «آر. إي. أم.» تساعد جهود الهند في الرقابة».
Wall Street Journal,
http://online.wsj.com/news/articles/SB100014240529702045053045770015923 35138870.

78. آلكسـاي أنيششوك (25 إبريل 2011). وكالة رويترز للأنباء. مقال: «شركة «بلاك بيري» تسعى إلى «التوازن» في روسيا»».
Reuters,
http://www.reuters.com/article/2011/04/25/us-blackberry-russia-idUSTRE73O1ZL20110425

79. قنـاة «الجزيـرة» التلفيزيونيّة. (4 أغسـطس 2010). مقال: «السـعوديّة تحظر «بلاك بـيري» بداية من يوم الجمعة»».
AlJazeera,
http://www.aljazeera.com/news/middleeast/2010/08/2010844243386999.html

80. صحيفة جاكرتا بوسـت (15 سـبتمبر 2011). مقال: «الحكومة تطلب من شركة «آر. آي. إم» نفاذاً مفتوحاً كي تتنصّت على مستخدمي «بلاك بيري»».
Jakarta Post,
http://www.thejakartapost.com/news/2011/09/15/government-asks-rim-open-access-wiretap-blackberry-users.html

81. جـوش هاليـداي (18 إبريل 2011). صحيفة الغارديان. مقال: «دولة الإمارات العربيّة المتحدة تشـدّد القيود على «بلاك بيري»».
Guardian,
http://www.theguardian.com/technology/2011/apr/18/uae-blackberrye-mails-secure

82. آر. جاي كريشـنا (8 أغسـطس 2012). صحيفة وول ستريت جورنال. مقال: «الهند تقترح اتفاقيّة للخلاف مع «بلاك بيري»».
Wall Street Journal,

http://online.wsj.com/news/articles/SB10000872396390443404004577576614174157698

«هيئة الإذاعة البريطانيّة» (11 يوليو 2013). مقال: «الهند «متأهّبة لاستعمال» نظام لاعتراض رسائل «بلاك بيري»».

BBC News,
http://www.bbc.com/news/technology-23265091.

83. جيمس بول وبنجامين غوتليب (25 سبتمبر 2012). صحيفة **الغارديان**. مقال: «إيران تشدّد الرقابة على الإنترنت بصنع شبكة خاصة بها».

Guardian,
http://www.theguardian.com/world/2012/sep/25/iran-state-run-internet

84. آتش. جي. أولبريخت (2003). بحث: «أولبريخت 2003: الحقيقة والكفاءة القانونيّتين لعمليّات اعتراض الاتصالات التي يشار إليها باسمي «100 أ» و«100 ب إس تي بي أو» وغيرها من إجراءات التحقيق: خلاصة». «معهد ماكس بلانك لقانون الجرائم الدولي والخارجي».

http://www.gesmat.bundesgerichtshof.de/gesetzesmaterialien/16_wp/telekueberw/rechtswirklichkeit_%20abschlussbericht.pdf.

85. ونستون ماكسويل وكريستوفر وولف (23 مايو 2012). بحث: «حقيقة عالميّة: نفاذ الحكومات إلى البيانات في السُّحُب الرقميّة: دراسة مقارنة لعشرة نُظُم قانونيّة دوليّة».

Hogan Lovells,
http://www.cil.cnrs.fr/CIL/IMG/pdf/Hogan_Lovells_White_Paper_Government_Access_to_Cloud_Data_Paper_1_.pdf.

86. «هيئة الإذاعة البريطانيّة» (20 نوفمبر 2012). أخبار «بي بي سي». مقال: «امرأة هنديّة مصدومة لاعتقالها بسبب تدوينة على «فيسبوك»».

BBC News,
http://www.bbc.com/news/world-asiaindia-20405457.

«وكالة الأنباء الفرنسيّة» (19 نوفمبر 2012). صحيفة **ساوث شاينا مورنينغ بوست**. مقال: «اعتقال هنود إثر تدوينات على «فيسبوك» عن إضراب مومباي».

Agence France-Presse (19 Nov 2012), «Indians arrested for Facebook post on Mumbai shutdown,» *South China Morning Post,*
http://www.scmp.com/news/asia/article/1086094/indians-arrested-facebook-post-mumbai-shutdown.

87. ديفيد ستوت (9 يوليو 2014). مجلة **تايم**. مقال: «الطغمة العسكريّة الحاكمة في تايلاند تعتقل مدرّساً بسبب تعليق على «فيسبوك»».

Time,
http://time.com/2968680/thailand-juntaeditor-facebook-thanapol-eawsakul-fah-diew-khan

88. «شبكة آسيا نيوز» (4 يونيو 2013). صحيفة **ستارتس تايمس**. مقال: «اعتقال امرأة بسبب تدوينة على «فيسبوك» عُدت مسيئة لملك ماليزيا».

http://news.asiaone.com/News/Latest+News/Science+and+Tech/Story/A1Story20130604-427357.html

89. من المحتمل أن حكومة أخرى كانت وراء الاختراق الأصلي، وأن الإيرانيّين امتطوا سطح ذلك النجاح. هانز هونغزستراتن وآخرون (13 أغسطس 2012). شركة «فوكس آي تي» مقال: «الـ«توليب» الأسود: تقرير عن اختراق «سلطة «ديجينوتار» للمصادقة».

http://www.rijksoverheid.nl/bestanden/documenten-en-publicaties/rapporten/2012/08/13/black-tulip-update/black-tulip-update.pdf.

90. سوميني سانغوبتا (11 سبتمبر 2011). صحيفة **نيويورك تايمس**. مقال: ««هاكر» يهزّ دوائر الأمن».

http://www.nytimes.com/2011/09/12/technology/hacker-rattles-internet-security-circles.html.

91. كريغ غايزر (6 سبتمبر 2011). مجلة عالم الكومبيوتر. مقال: «تجسّس «هاكرز» على 300 ألف عنوان بريد إلكتروني إيراني في «جي ميل» باستخدام مصادقة مزيّفة من «غوغل»».
Computer World,
http://www.computerworld.com/s/article/9219731/Hackers_spied_on_300_000_Iranians_using_fake_Google_certificate.

92. «مرصد أسلحة المعلوماتيّة». جامعة تورنتو، «مختبر المواطن»، «مركز مونك للدراسات الدوليّة». بحث: «تتبّع «غوست نت»: تحقيق عن شبكة تجسّس سبراني».
http://www.infowar-monitor.net/ghostnet.

93. إلين ناكاشيما (28 مايو 2012). صحيفة واشنطن بوست. مقال: «فيروس كومبيوتر يستخدم للتجسّس، ويفوق فيروس «ستاكس نت» بعشرين ضعفاً».
Washington Post,
http://www.washingtonpost.com/world/national-security/newly-identified-computer-virus-used-for-spying-is-20-times-size-of-stuxnet/2012/05/28/gJQAWa3VxU_story.html.

94. دان غودين (14 يناير 2013). موقع «آرس تكنيكا». مقال: «برنامج خبيث للتجسّس المكثف استمر في التجسّس على الحكومات بخفاء لـ5 سنوات».
Ars Technica,
http://arstechnica.com/security/2013/01/red-Oct-computer-espionage-network-may-have-stolen-terabytes-ofdata

95. بيتر آبس وجيم فينكل (7 مارس 2014). وكالة «رويترز» للأنباء. مقال: «برنامج تجسّس روسي اسمه «تورلا»، استهدف أوروبا والولايات المتحدة».
Reuters,
http://www.reuters.com/article/2014/03/07/us-russia-cyberespionage-insight-idUSBREA260YI20140307

96. مختبر شركة «كاسبارسكي» (10 فبراير 2014). «إماطة اللثام عن «كاريتو»: فيروس التطبيقات المقنّع».
Securelist,
http://www.securelist.com/en/downloads/vlpdfs/unveilingthemask_v1.0.pdf

97. إلين ناكاشيما (29 مايو 2014). صحيفة واشنطن بوست. مقال: ««هاكرز» إيرانيّون استهدفوا رسميّين أميركيّين».
Washington Post,
http://www.washingtonpost.com/world/national-security/iranian-hackers-are-targeting-us-officials-through-social-networksreport-says/2014/05/28/7cb86672-e6ad-11e3-8f90-73e071f3d637_story.html

98. ماثيو م. إيد (10 يونيو 2013). مجلة فورين بوليسي. مقال: «في دواخل المجموعة الأشد سريّة في «وكالة الأمن القومي» لاختراق الصين».
Foreign Policy,
http://www.foreignpolicy.com/articles/2013/06/10/inside_the_nsa_s_ultra_secret_china_hacking_group.

99. بروس شناير (4 أكتوبر 2013). صحيفة الغارديان. مقال: «الهجوم على برنامج «تور»: كيف استهدفت «وكالة الأمن القومي» إخفاء الهويّة لمستخدمي الإنترنت».
Guardian,
http://www.theguardian.com/world/2013/oct/04/tor-attacks-nsa-users-online-anonymity

100. الأسماء الشيفريّة لتلك البرامج مسليّة تماماً. وما يثير أشد الاهتمام أنّ تلك الوثيقة العالية السريّة لـ«وكالة

الأمن القومي»، لم تأتِ من إدوارد سنودن. موقع «ليك سورس» (30 ديسمبر 2013). وثيقة: «دليل إرشادي من «قسم مكافحة الإرهاب» في «وكالة الأمن القومي» يظهر كيفيّة استغلال معظم البرمجيّات الرقميّة الكبرى، وكذلك الحال بالنسبة للمكوّنات الإلكترونيّة وبرمجيّات الشركات».

http://leaksource.info/2013/12/30/nsas-ant-division-catalog-of-exploits-for-nearly-every-major-software-hardware-firmware

صحيفة دير شبيغيل (29 ديسمبر 2013). مقال: «دواخل مجموعة «تاو»: وثيقة تكشف المجموعة الأكثر تقدّماً في اختراق الكومبيوتر لدى «وكالة الأمن القومي».

Der Spiegel,

http://www.spiegel.de/international/world/the-nsa-uses-powerful-toolbox-in-effort-to-spy-on-global-networks-a-940969.html.

جاكوب آبلباوم، جوديث هورشيرت وكريستيان ستوكر (29 ديسمبر 2013). صحيفة دير شبيغيل، مقال: «تسوّق خدمة لأداة تجسّس: كاتالوغ يشرح صندوق العدّة عند «وكالة الأمن القومي»».

Der Spiegel,

http://www.spiegel.de/international/world/catalog-reveals-nsa-has-back-doorsfor-numerous-devices-a-940994.html.

101. ماثيو م. آيد (15 أكتوبر 2013). مجلة فورين بوليسي. مقال: «محطّمو الشيفرة الجدد لدى «وكالة الأمن القومي»».

Foreign Policy,

http://www.foreignpolicy.com/articles/2013/10/15/the_nsa_s_new_codebreakers

102. يتضمن المقال التالي وصفاً لإحدى الوحدات الصينيّة العسكريّة لاختراق الكومبيوتر. مانديانت (18 فبراير 2013). مقال: «إي بي تي 1»: عرض لإحدى أضخم وحدات التجسّس السبراني في الصين».

http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf.

103. كيم زيتر (13 يناير 2010). مجلة وايرد. مقال: «مخترقو نظام «غوغل» استهدفوا شيفرة المصدر في ما يزيد على 30 شركة».

Wired,

http://www.wired.com/2010/01/google-hack-attack

104. غريغ ويستون (16 فبراير 2011). شبكة «سي بي سي نيوز». مقال: «الحكومة الكنديّة استهدفها «هاكرز» أجانب».

CBC News,

http://www.cbc.ca/news/politics/foreign-hackers-attack-canadian-government-1.982618

105. نيكول برلروث (31 يناير 2013). صحيفة نيويورك تايمس. مقال: «مجموعة «هاكرز» من الصين هاجمت نيويورك تايمس خلال الشهور الـ4 الماضية».

New York Times,

http://www.nytimes.com/2013/01/31/technology/chinese-hackers-infiltrate-new-york-times-computers.html.

106. آلين ناكاشيما (19 مايو 2014). صحيفة واشنطن بوست. مقال: «الولايات المتحدة تعلن أول تهمة ضد بلد أجنبي بصدد التجسّس السبراني».

Washington Post,

http://www.washingtonpost.com/world/national-security/us-to-announce-firstcriminal-charges-against-foreign-country-for-cyberspying/2014/05/19/586c9992-df45-11e3-810f-764fe508b82d_story.html

107. ريفا ريتشموند (2 أبريل 2011). صحيفة نيويورك تايمس. «كيف تمكّن الـ«هاكرز» من اختراق شركة «آر أس إيه»».

http://bits.blogs.nytimes.com/2011/04/02/the-rsahack-how-they-did-it.

Kelly Jackson Higgins (29 Mar 2012), «China hacked RSA, U.S. official says,»

Information Week,
http://www.darkreading.com/attacks-breaches/china-hacked-rsa-us-official-says/d/d-id/1137409

108. جوليـان إي. بارنز (4 مارس 2008). صحيفة **لوس أنجلوس تايمس**. مقال: «البنتاغون قلق من نشـاطات الصين في اختراق الكومبيوتر».
Los Angeles Times,
http://articles.latimes.com/2008/mar/04/world/fg-uschina4
آلين ناكاشيما (17 مايو 2013). صحيفة **واشنطن بوست**. مقال: «تقرير سري يعدّد نظم التسليح الأميركيّة التي اخترقها جواسيس الفضاء السبراني الصينيّون».
Washington Post,
http://www.washingtonpost.com/world/national-security/confidential-report-lists-us-weapons-system-designs-compromised-by-chinese-cyberspies/2013/05/27/a42c3e1cc2dd-11e2-8c3b-0b5e9247e8ca_story.html.

109. لا نعـرف إن كانـت الحكومة الصينيّة تقف وراء تلك البرمجيّات، لكن الحيثيّات المرافقة لها تبدو كافية للإدانة. آنـدي غرينبرغ (1 أبريـل 2013). مجلة **فوربس**. مقال: «أدلة متراكمة عن وقوف «هاكرز» الحكومة الصينيّة وراء برمجيّات خبيثة في هواتف «آندرويد»».
Forbes,
http://www.forbes.com/sites/andygreenberg/2013/04/01/evidencemounts-that-chinese-government-hackers-spread-android-malware

110. آلين ناكاشـيما وليزا راين (11 يوليو 2014). صحيفة **واشـنطن بوسـت**. مقال: «اختراق صيني يسـتهدف بيانات موظفين حكوميّين أميركيّين».
Washington Post,
http://www.washingtonpost.com/world/national-security/chinese-hackers-go-after-us-workers-personaldata/2014/07/10/92db92e8-0846-11e4-8a6a-19355c7e870a_story.html

111. بيتر شـفايزر (يناير/فبرايـر 1996). مجلة **فورين آفيرز**. مقال: «تصاعد التجسّـس الاقتصادي: أميركا هي الهدف رقم 1».
Foreign Affairs,
http://www.foreignaffairs.com/articles/51617/peter-schweizer/the-growth-of-economic-espionageamerica-is-target-number-one.

112. ديفيد سانغر (20 مايو 2014). صحيفة **نيويورك تايمس**. مقال: «عبر تهم بالتجسّس، الولايات المتحدة تشدّ خيطاً مرهفاً ضد التجسّس الصيني».
New York Times,
http://www.nytimes.com/2014/05/20/us/us-treads-fine-line-in-fighting-chinese-espionage.html.
جاك غولد سميث (25 مايو 2013). مجلة **لو فاير**. مقال: «سبب وهن الاتهام الأميركي للصين بالتجسّس».
Jack Goldsmith (25 Mar 2013), «Why the USG complaints against Chinese eco- nomic cyber-snooping are so weak,» *Lawfare*,
http://www.lawfareblog.com/2013/03/why-the-usg-complaints-against-chinese-economic-cyber-snooping-are-so-weak.

113. صحيفة **أو غلوبو** (8 سبتمبر 2013). مقال: «وثائق «وكالة الأمن القومي» تظهر تجسّساً أميركيّاً على عملاق النفط البرازيلي».
O Globo,
http://g1.globo.com/fantastico/noticia/2013/09/nsa-documents-show-united-states-spied-brazilian-oil-giant.html

114. صحيفة دير شـبيغيل (15 سـبتمبر 2013). مقال: «تتبّـع المال: «وكالة الأمن القومي» تتجسّـس على نظام «سويفت» للمعاملات الماليّة العالميّة».

Der Spiegel,
http://www.spiegel.de/international/world/spiegel-exclusive-nsa-spies-on-international-bank-transactions-a-922276.html

115. كينيث دبليو دام وهربرت لين، كتاب دور التشـفير في تأمين معلومات المجتمع (1996). (دار «ناشـيونال أكاديميز برس»).

http://www.nap.edu/catalog.php?record_id=5131.

116. مورغان- ماركيز بوار وآخرون (24 يونيو 2014). جامعة تورنتو، «مختبر المواطن»، «مركز مونك للدراسات الدوليّة». مقال: «قصة بوليسيّة: برنامج خبيث للتجسّس الحكومي صنعته 'هاكينغ تيم'».

Citizen Lab, Munk School of Global Affairs, University of Toronto,
https://citizenlab.org/2014/06/backdoor-hacking-teams-tradecraft-android-implant.
William Anderson (24 Jun 2014), «Hacking Team 2.0: The story goes mobile,» Securelist,
http://securelist.com/blog/research/63693/hackingteam-2-0-the-story-goes-mobile

117. بيل ماركزاك وآخرون. (12 فبراير 2014). جامعة تورنتو، «مختبر المواطن»، «مركز مونك للدراسات الدوليّة». مقال: «شركة «هاكينغ تيم» واستهداف الصحافيّين الإثيوبيّين».

https://citizenlab.org/2014/02/hacking-team-targeting-ethiopian-journalists

كريغ تيمبرغ (12 فبراير 2014). صحيفة واشـنطن بوسـت. مقال: «نُظُم حكم أجنبيّة تسـتخدم برمجيّات تجسّس على الصحافيّين، حتى في الولايات المتحدة».

Washington Post,
http://www.washingtonpost.com/business/technology/foreign-regimes-use-spyware-against-journalistseven-in-us/2014/02/12/9501a20e-9043-11e3-84e1-27626c5ef5fb_story.html

118. آنـدرو جاكوبـس، مغويـل هيلفت وجون ماركـوف (13 يونيـو 2010). صحيفة نيويـورك تايمس. مقال: ««غوغل» يحدّد مصدر الهجمات، ويهدّد بمغادرة الصين».

New York Times,
http://www.nytimes.com/2010/01/13/world/asia/13beijing.html

ديفيد إي. سـانغر (6 مايو 2013). صحيفة نيويورك تايمس. مقال: «الولايات المتحدة تلقي باللوم مباشرة على الجيش الصيني بخصوص هجمات في الفضاء السبراني».

New York Times,
http://www.nytimes.com/2013/05/07/world/asia/us-accuses-chinas-military-incyberattacks.html

119. صحيفة نيويورك تايمس (7 مايو 2013). افتتاحيّة: «الصين والحرب السبرانيّة».

New York Times,
http://www.nytimes.com/2013/05/08/opinion/china-and-cyberwar.html.

ديفيد سـانغر وإليزابيث بوميلر (31 مايو 2011). صحيفة نيويورك تايمس. مقال: «البنتاغون سـيصنّف هجمات الفضاء السبراني أفعالاً حربيّة».

New York Times.
http://www.nytimes.com/2011/06/01/us/politics/01cyber.html.

120. بـاراك أوباما (17 يناير 2014). صحيفة نيويورك تايمس. مقال: «خطاب أوباما عن تجسّـس «وكالة الأمن القومي» على الهواتف».

New York Times,
http://www.nytimes.com/2014/01/18/us/politics/obamas-speech-on-nsa-phone-surveillance.html.

121. مايكل س. سـميث، كيث برادشـير وكريسـتين هاوزر (8 أكتوبر 2012). صحيفة **نيويورك تايمس**. مقال: «لجنة أميركيّة تجد مخاطر في معدّات صينيّة».
http://www.nytimes.com/2012/10/09/us/us-panel-calls-huawei-and-zte-national-security-threat.html

122. «وكالة الأمن القومي» (24 يونيو 2008). وثيقة: «سوفلترو: بيانات المنتَج عن مجس «إيه أن تي» اللاسلكي».
http://leaksource.files.wordpress.com/2013/12/nsa-ant-souffletrough.jpg
«وكالة الأمن القومي» (24 يونيو 2008). وثيقة: «فيد- ثرو»: بيانات المنتَج عن مجس «إيه أن تي» اللاسلكي».
http://leaksource.files.wordpress.com/2013/12/nsa-ant- feedthrough.jpg
«وكالة الأمن القومي» (24 يونيو 2008). وثيقة: «جيت بلو»: بيانات المنتَج عن مجس «إيه أن تي» اللاسلكي».
http://leaksource.files.wordpress.com/2013/12/nsa-ant-jetplow.jpg.
«وكالة الأمن القومي» (24 يونيو 2008). وثيقة: «هيد ووتر»: بيانات المنتَج عن مجس «إيه أن تي» اللاسلكي».
http://leaksource.files.wordpress.com/2013/12/nsa-ant-headwater.jpg.
«وكالـة الأمـن القومي» (24 يونيـو 2008). وثيقة: «هالوكـس ووتر»: بيانات المنتَج عـن مجس «إيه أن تي» اللاسلكي».
http://leaksource.files.wordpress.com/2013/12/nsa-ant-halluxwater.jpg.

123. جيرمي هسو (26 مارس 2014). مقال: «شكوك الولايات المتحدة بـ«هواوي» الصينيّة تستند أساساً إلى الخدع التي تمارسها «وكالة الأمن القومي» نفسها».
IEEE Spectrum,
http://spectrum.ieee.org/tech-talk/computing/hardware/us-suspicions-of-chinas-huawei-based-partly-on-nsas-own-spy-tricks.

124. في التعابير العسـكريّة، يسـمّى الاختراق بهدف التجسّـس «تسلّل إلى شـبكة كومبيوتر من الخارج»، ويختصر بمصطلـح «سي آن إي» (*CNE*)، ويسـمّى الاخـتراق بهـدف إلحـاق ضرر بالكومبيوتـر «هجـوم على شـبكة حواسيب»، ويختصر بمصطلح «سي آن إيه» (*CNA*). آلكسندر كليمبرغ وهيلي تيرما- كلار (15 أبريل 2011). دراسـة: «الأمن السبراني والقوة السـبرانيّة: المفاهيم والشروط والقدرات بهدف التعاون للعمل داخل «الاتحاد الأوروبي»».
Directorate-General for External Policies of the Union,
http://www.europarl.europa.eu/RegData/etudes/etudes/join/2011/433828/EXPO-SEDE_ET(2011)433828_EN.pdf.
Alexander Klimburg (2 Sep 2014), «Shades of cyber grey: Espionage and attack in cyberspace,» *Fletcher Forum of World Affairs*,
http://www.fletcherforum.org/2014/09/02/klimburg

125. ولكن ذلك لا يمثّل «حرباً سـبرانيّة»، على الرغم من شيوع استعمال ذلك المصطلح في الخطاب السياسي. لتجنّب الخلـط بين الأمرين، يمكن قراءة الكتاب التالي: **الحرب السـبرانيّة لن تحدث أبـداً** (2013)، تأليف: توماس ريد، «مطبعة جامعة أوكسفورد».
http://thomasrid.org/no-cyber-war

126. جيمس بامفورد (13 أغسطس 2014). مجلة وايرد. مقال: «إدوارد سنودن: القصة غير المعلنة».
Wired,
http://www.wired.com/2014/08/edward-snowden

127. يملك عدد أكبر من البلدان قدرات في الحرب السبرانيّة. كليّة السياسة العامة في «جامعة جورج ماسون» (فبراير 2014). دراسة: «أسواق تصدير الأمن السبراني». «شراكة فرجينيا للتنمية الاقتصادية».
http://exportvirginia.org/wp-content/uploads/2014/02/Report-on-Cyber-Security-Preface.pdf

128. جوشـوا ديفيز (21 أغسطس 2007). مجلة وايرد. مقال: «الـ«هاكرز» يضربون البلد الأكثر اتّصالاً بالإنترنت في أوروبا».
Wired,

https://web.archive.org/web/20071019223411/http://www.wired.com/politics/security/magazine/15-09/ff_estonia

129. جون ماركوف (13 أغسطس 2008). صحيفة **نيويورك تايمس**. مقال: «الهجمات السبرانيّة سبقت الحرب الفعليّة».

New York Times

http://www.nytimes.com/2008/08/13/technology/13cyber.html.

130. ماثيو ويبفر (8 يوليو 2009). صحيفة **الغارديان**. مقال: «هجمات سبرانيّة تستهدف كوريا الجنوبيّة والولايات المتحدة».

Guardian,

http://www.theguardian.com/world/2009/jul/08/south-korea-cyber-attack

131. تشارلز كلوفر (11 مارس 2009). صحيفة **فايننشال تايمس**. مقال: «مجموعة يساندها الكرملين مسؤولة عن الهجمات السبرانيّة على أستونيا».

Financial Times,

http://www.ft.com/cms/s/0/57536d5a-0ddc-11de-8ea3-0000779fd2ac.html

132. مجلة كومبيوتر ويكلي (13 مارس 2009). مقال: «صغار السن مسؤولون عن هجمات أستونيا».

Computer Weekly,

http://www.computerweekly.com/news/2240088733/Kids-responsible-for-Estonia-attack

133. ديفيد كوشنر (26 فبراير 2013). مقال: «القصة الحقيقيّة لـ«ستاكس نت»».

IEEE Spectrum,

http://spectrum.ieee.org/telecom/security/the-realstory-of-stuxnet

كيم زيتر (2014). كتاب **العدّ العكسي لليوم صفر: «ستاكس نت» وإطلاق أول سلاح رقمي في العالم**. دار «كراون بابليشرز».

http://books.google.com/books/?id=iBTpnQEACAAJ.

134. ويليام جي. برود، جون ماركوف وديفيد ي. سانغر (15 يناير 2011). صحيفة **نيويورك تايمس**. مقال: «تجربة إسرائيليّة على دودة إلكترونيّة أدّت لتأخير في برنامج إيران النووي».

New York Times,

http://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html

135. نيكول بيلروث (23 أكتوبر 2012). صحيفة **نيويورك تايمس**. مقال: «في الهجوم السبراني على «آرامكو»، الولايات المتحدّة رأت ردّاً إيرانياً».

New York Times,

http://www.nytimes.com/2012/10/24/business/global/cyberattack-on-saudi-oil-firm-disquiets-us.html.

وكالة أنباء «رويترز» (9 ديسمبر 2012). صحيفة **نيويورك تايمس**. مقال: «شركة «آرامكو» تقول إن هجوماً سبرانياً استهدف إنتاجها».

New York Times,

http://www.nytimes.com/2012/12/10/business/global/saudi-aramco-says-hackers-took-aim-at-its-production.html

136. دريك س. ريفرون. (صيف 2008). بحث: «مكافحة الإرهاب والتعاون الاستخباراتي». **مجلة التغيير العالمي والحوكمة** العدد 1.

http://www.globalaffairsjournal.com/archive/Summer08/REVERON.pdf.

137. روس أندرسون (23-24 يونيو 2014). جامعة بنسلفانيا. بحث: «الخصوصيّة في مواجهة رقابة الحكومة: تقابل آثار الشبكة مع خيار الناس».

13th Annual Workshop on the Economics of Information Security, Pennsylvania State University,

http://weis2014.econinfosec.org/papers/Anderson-WEIS2014.pdf.

138. نيك بيري وبايزلي دودز (16 يوليو 2013)، وكالة «أسوشيتد برس»، مقال: «تحالف الأمم الخمسة كان محورياً في الأذى الذي سبّبته التسريبات».

Associated Press,

http://bigstory.ap.org/article/expertssay-us-spy-alliance-will-survive-snowden.

139. هنريك مولتكه وغياردنغ (4 نوفمبر 2013). مقال: «الدانمارك جزء من الحلقة الداخلية لـ«وكالة الأمن القومي».

Information,

http://www.information.dk/477405

140. مجلة دير شبيغيل (22 يوليو 2013). مقال: «شركاء أساسيّين: تحالف محوري بين ألمانيا والولايات المتحدة».

Der Spiegel,

http://www.spiegel.de/international/world/german-intelligence-worked-closely-with-nsa-on-data-surveillance-a-912355.html

هربرت غوديه وآخرون. (18 يونيو 2014). صحيفة دير شبيغيل. مقال: «لنتجسّس معاً: التعاون العميق بين ألمانيا و«وكالة الأمن القومي»».

Der Spiegel,

http://www.spiegel.de/international/germany/thegerman-bnd-and-american-nsa-cooperate-more-closely-than-thought-a-975445.html

141. إيوين ماكآسكل وجيمس بول (2 نوفمبر 2013). صحيفة الغارديان. مقال: «بورتريه عن «وكالة الأمن القومي»: لا هدف أصغر من أن يلاحظ، للتوصّل إلى الرقابة الشاملة».

http://www.theguardian.com/world/2013/nov/02/nsa-portrait-total-surveillance.

142. جاي سولومن وسيوبهان غورمان (9 مايو 2012). صحيفة وول ستريت جورنال. مقال: «خلف إحباط مخطط الطائرة النفّاثة».

Wall Street Journal,

http://online.wsj.com/news/articles/SB10001424052702304543904577394373945627482

غلين غرينوالد ومرتضى حسين (25 يوليو 2014). موقع «إنترسيبت». مقال: «شريك جديد لوكالة الأمن القومي».

Intercept,

https://firstlook.org/theintercept/2014/07/25/nsas-new-partner-spying-saudi-arabias-brutal-state-police

143. إدوارد سنودن (7 مارس 2014). «بيان إلى برلمان «الاتحاد الأوروبي»».

European Parliament,

http://www.europarl.europa.eu/document/activities/cont/201403/20140307ATT80674/20140307ATT80674EN.pdf.

144. آندي مولر ماكغون وآخرون (31 أغسطس 2014). صحيفة دير شبيغيل. مقال: «صداقة بوجه مزدوج: تركيا هي «الشريك والهدف» بالنسبة لـ«وكالة الأمن القومي»».

Der Spiegel,

http://www.spiegel.de/international/documents-show-nsa-and-gchq-spied-on-partner-turkey-a-989011.html.

لورا بواتراس وفريقها (31 أغسطس 2014). موقع «إنترسيبت». مقال: «كيف ساعدت «وكالة الأمن القومي» تركيا في قتل المتمرّدين الأكراد».

Intercept,

https://firstlook.org/theintercept/2014/08/31/nsaturkeyspiegel

145. ديفيد إي. سانغر (1 مايو 2014). صحيفة نيويورك تايمس. مقال: «الولايات المتحدة وألمانيا تفشلان في الاتفاق بشأن التجسّس».

New York Times,

http://www.nytimes.com/2014/05/02/world/europe/us-and-germany-fail-to-reach-a-deal-on-spying

مـارك لاندر (2 آيار 2014). صحيفة نيويورك تايمس. مقال: «ميركل تشـير إلى اسـتمرار التوتر مع أميركا بشأن التجسّس».

New York Times,
http://www.nytimes.com/2014/05/03/world/europe/merkelsays-gaps-with-us-over-surveillance-remain.html.

آندي موللر- ماغوهن وآخرون (14 سـبتمبر 2014). صحيفة دير شـبيغيل. «خريطة الكنز: انتهاك «وكالة الأمن القومي» لـ«شركة تلكوم» وغيرها من الشركات الألمانيّة».

Der Spiegel,
http://www.spiegel.de/international/world/snowden-documents-indicatensa-has-breached-deutsche-telekom-a-991503.html

146. يعتقـد كثيرون بأن الولايات المتحدة والمملكة المتحدة تتجسّسـان كلٌ على مواطني الأخرى، بهدف الالتفاف على قوانين البلدين. ويكون ذلك شرعياً بمقدار ما تقدران على إقناع نفسيهما بأن «لا مفر منها».

147. جوسـتان إليوت وثيودوريك مييار (11 سـبتمبر 2013). موقع «بروبابليكا». مقال: «مزاعم بأن «وكالة الأمن القومي» «أحبطت مخطّطاً «ينتشر على الرغم من غياب الأدلة».

Pro Publica,
http://www.propublica.org/article/claim-on-attacks-thwarted-by-nsa-spreads-despitelack-of-evidence.

148. غلين غرينوالد، لورا بواتراس وإيون ماكآسـكل (11 سبتمبر 2013). صحيفة الغارديان. مقال: ««وكالة الأمن القومي» تشارك إسرائيل معلومات استخباراتيّة خاما، ضمنها بيانات عن أميركيّين».

Guardian,
http://www.theguardian.com/world/2013/sep/11/nsa-americans-personal-dataisrael-documents.

149. لا تزال الاعتبارات السياسيّة مهمة. تملك الصين مشكلة كبيرة مع إرهابيّي الـ«إيغور»، وسترحّب بأن تساعدها أمـيركا في التعامـل مع ذلك التهديد. وبالطبع، تمتنع أميركا عن مسـاعدتها؛ لأن إرهاب الـ«إيغور» يسـاهم في إضعاف الصين. شـيان- بينغ شـونغ (2002). مجلـة فورين آفيرز. مقال: «حرب الصـين على الإرهاب: 11 سبتمبر والانفصاليون الـ«إيغور»».

Foreign Affairs,
http://www.foreignaffairs.com/articles/58030/chien-peng-chung/chinas-war-on-terror-september-11-and-uighur-separatism

إليزابيث فان ووي ديفيس (يناير 2008). «مركز دراسـات الأمن لمنطقة آسـيا- المحيط الهادئ». بحث: «إثنيّة الـ«إيغور» المسلمة الانفصالية في «زينجيانغ»، الصين».

http://www.apcss.org/college/publications/uyghur-muslim-ethnic-separatism-in-xinjiang-china

150. جون لافلاند (8 سبتمبر 2004). صحيفة الغارديان. مقال: «الشيشان أصدقاء أميركا».

Guardian,
http://www.theguardian.com/world/2004/sep/08/usa.russia

سيمون شوستر (19 سبتمبر 2011). مجلة تايم. «كيف استفادت روسيا من الحرب على الإرهاب».

Guardian,
http://www.theguardian.com/world/2004/sep/08/usa.russia

جيمـس جـوردن مييـك (19 فبراير 2014). شـبكة «إيه بي سي نيوز». مقـال: «المعارك السريّـة بين القوات الأميركيّة وإرهابيّي الشيشان».

«The secret battles between US forces and Chechen terrorists,» *ABC News*,
http://abcnews.go.com/Blotter/secret-battles-usforces-chechen-terrorists/story?id=22580688

151. توم وينتر (25 مارس 2014). شبكة «آن بي سي نيوز». مقال: «روسيا حذّرت أميركا من تسارناييف، لكنه أفلت بسبب أخطاء في التهجئة».
NBC News,
http://www.nbcnews.com/storyline/boston-bombing-anniversary/russia-warned-u-s-about-tsarnaevspelling-issue-let-him-n60836

152. لورا سميث- سبارت ونيك باتون والش (4 فبراير 2014). شبكة «سي آن آن». مقال: «أميركا تكشف «تهديدات محدّدة» لـ«دورة سوتشي الأولمبيّة»».
CNN,
http://www.cnn.com/2014/02/04/world/europe/russia-sochi-winter-olympics

الفصل 6 : تعزيز السيطرة المؤسّساتيّة

1. وصف أستاذ الاتصالات البروفسور روبرت م. ماكشيسني ذلك التحالف بأنّه علاقة اعتماد متبادل بين الحكومات الضخمة والبيانات الضخمة؛ لأنه «زواج عقد في السماء، مع إملاءات مريرة على الحريّة والديمقراطيّة». روبرت م. ماكشيسني (2013). كتاب: **الانفصال الرقمي: كيف تستخدم الرأسماليّة الإنترنت ضد الديمقراطيّة.** دار «نيو برس».
http://books.google.com/books/?id=j_7EkTI8kVQC
كنّا نعرف عن ذلك حتى قبل سنودن، بفضل مارك كلاين، وهو أحد مطلقي صافرة الإنذار ضد «وكالة الأمن القومي». مارك كلاين (8 يونيو 2006). «إعلان مارك كلاين».
Hepting, et al., v. AT&T, et al., United States District Court, Northern District of California (No. C-06-0672-VRW),
https://www.eff.org/files/filenode/att/Mark%20Klein%20Unredacted%20Decl-Including%20Exhibits.pdf
آلين ناكاشيما (7 نوفمبر 2007). صحيفة **واشنطن بوست.** مقال: «قصة رقابة».
Washington Post,
http://www.washingtonpost.com/wp-dyn/content/article/2007/11/07/AR2007110700006.html
جيمس بول، لوك هاردينغ وجوليات غارسايد (2 أغسطس 2013). صحيفة **الغارديان.** مقال: «شركتا «بي تي» و«فودافون» بين شركات اتصالات تقدّم تفاصيل إلى «القيادة الحكوميّة للاتّصالات»».
http://www.theguardian.com/business/2013/aug/02/telecoms-bt-vodafonecables-gchq.

4. «فودافون» (2014). وثيقة: «تقرير عن كشف المعلومات إلى قوى إنفاذ القانون».
report, http://www.vodafone.com/content/sustainabilityreport/2014/index/operating_responsibly/privacy_and_security/law_enforcement.html
جوليات غارسايد (5 يونيو 2014). صحيفة **الغارديان.** مقال: ««فودافون» تكشف وجود خطوط سريّة تتيح رقابة الحكومة».
Guardian,
http://www.theguardian.com/business/2014/jun/06/vodafone-reveals-secretwires-allowing-state-surveillance

5. جاك فلورو وغلين غرينوالد (25 أكتوبر 2013). صحيفة **لو موند.** مقال: «فرنسا في مقعد مشترك مع «وكالة الأمن القومي»: استهداف «وانادو» و«آلكاتيل»».
Le Monde,
http://www.lemonde.fr/technologies/article/2013/10/21/france-in-the-nsa-s-crosshair-wanadoo-and-alcatel-targeted_3499739_651865.html

جاك فلورو (21 مارس 2014)، صحيفة لو موند، مقال: «تجسّس: كيف تعاونت شركة «أورانج» مع الاستخبارات السريّة».
Le Monde,
http://www.lemonde.fr/international/article/2014/03/20/dgse-orange-des-liaison sincestueuses_4386264_3210.html

6. هيئة الإذاعة البريطانيّة (8 إبريل 2014). «بي بي سي نيوز». «المحكمة العليا في «الاتحاد الأوروبي» ترفض قانون الاحتفاظ بالبيانات في دول «الاتحاد الأوروبي»».
BBC News,
http://www.bbc.com/news/world-europe-26935096.

7. برنامج الإعلام في إيران (8 أبريل 2013). «الإعلام الرقمي: سلطات الاتصالات تراقب مقاهي الإنترنت بواسطة 20 قانوناً جديداً».
Annenberg School for Communication,
http://www.iranmediaresearch.org/en/blog/218/13/04/08/1322

8. «مراسلون بلا حدود» (2013). فصل عن فيتنام في كتاب **أعداء الإنترنت**.
http://surveillance.rsf.org/en/vietnam

9. راما لاكشمي (1 أغسطس 2011). صحيفة **واشنطن بوست**. مقال: «انتقاد قوانين الهند الجديدة عن الإنترنت».
Washington Post,
http://www.washingtonpost.com/world/indias-new-internet-rules-criticized/2011/07/27/gIQA1zS2mI_story.html.

10. كريس غاي هوناغل (1 أغسطس 2003). مقال: «المساعدون الصغار لـ«الأخ الكبير»: كيف تعمل شركة «تشويس بوينت» وغيرها من سماسرة المعلومات، على جمع بياناتك وتجهيزها لمصلحة قوى إنفاذ القانون».
North Carolina Journal of International Law and Commercial Regulations 29, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=582302.
جون د. ميكايلز (6 أكتوبر 2008). مقال: «كل جواسيس الرئيس: شراكات بين الاستخبارات الخاصة والعامة في الحرب على الإرهاب».
California Law Review 96,
http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1279867.

11. ماثيو ل. والد (21 فبراير 2004). صحيفة **نيويورك تايمس**. مقال: «الولايات المتحدة تصف نشر بيانات شركة «جيت بلو» بأنه غير مناسب».
New York Times,
http://www.nytimes.com/2004/02/21/business/21blue.html.

12. «سي آر ستاف» (1 مايو 2003). «الحكومة الأميركيّة تشتري بيانات 65 ناخباً مكسيكيا مسجلاً». مركز «إنفورميشين كليرنغهاوس».
http://www.informationclearinghouse.info/article3186.htm.

13. «الشبكة الأميركيّة لدعم مكافحة الجرائم الماليّة» (11 مايو 2014). «متطلّبات قانون السريّة المصرفيّة: مرجع سريع عن الخدمات الماليّة».
http://www.fincen.gov/financial_institutions/msb/materials/en/bank_reference.html

14. كينيث لوي (29 يونيو 2008). صحيفة **هيرالد ريفيو**. «حصلت «إيلينوي» على 64.3 مليون دولار من بيع بيانات رخص السواقة».
Herald-Review,
http://herald-review.com/business/local/illinois-made-million-selling-driver-s-license-information/article_43c51a15-c885-575e-ac5d-0c01cc9acb6b.html

15. جوي غولين (11 يوليو 2010). مقال: «ولاية أوهايو تكسب ملايين الدولارات من بيع بيانات رخص القيادة مرفقة ببياناتك الشخصيّة». موقع «بلين ديلار».

Plain Dealer,
http://www.cleveland.com/open/index.ssf/2010/07/ohio_collects_millions_selling.html

16. تيم كاشينغ (13 فبراير 2013). موقع «تيك ديرت». مقال: «ولاية «تكساس» تبيع المعلومات الشخصيّة إلى مئات الشركات، والسائقون غير مسموح لهم بالامتناع».

Tech Dirt,
http://www.techdirt.com/articles/20130212/21285321958/texas-dmv-sells-personal-information-to-hundreds-companies-drivers-not-allowed-to-opt-out.shtml.

17. جيف فاينزير (12 أكتوبر 2011). مقال: «ولاية فلوريدا تكسب 63 مليون دولار من بيع معلومات عن السائقين».

Local 10,
http://www.local10.com/news/Florida-Makes-63M-Selling-Drivers-Info/3078462

18. كيم زيتير (11 ديسمبر 2003). مجلة وايرد. مقال: «معروض للبيع: الناخب الأميركي».

Wired,
http://archive.wired.com/politics/security/news/2003/12/61543

19. روبنا ماكسون (18 إبريل 2014). صحيفة الغارديان. مقال: «الحكومة البريطانيّة تبيع البيانات الماليّة لدافعي الضرائب».

Guardian,
http://www.theguardian.com/politics/2014/apr/18/hmrc-to-sell-taxpayers-data

20. رانديب راميش (19 يناير 2014). صحيفة الغارديان. مقال: ««الخدمات الصحيّة الوطنيّة» تجعل بيانات المرضى متاحة لشركات الأدوية والضمان».

Guardian,
http://www.theguardian.com/society/2014/jan/19/nhs-patient-data-available-companies-buy

21. سُمّي ذلك «تبييض المعلومات». كريس غاي هوفناغل (2 سبتمبر 2014). موقع «سلايت». مقال: «المخادعة الإيحائيّة في الخصوصيّة البراغماتيّة».

Slate,
http://www.slate.com/articles/technology/future_tense/2014/09/data_use_regulation_the_libertarian_push_behind_a_new_take_on_privacy.single.html.

22. جيوف دونكان (9 يونيو 2012). موقع «ديجيتال تريندز». مقال: «لماذا لا يحمي خيار عدم التتبّع إلى خصوصيّة الأشخاص».

Digital Trends,
http://www.digitaltrends.com/mobile/why-do-not-track-may-not-protect-anybodys-privacy

23. البرلمان الأوروبي والمجلس الأوروبي (24 أكتوبر 1995). «توجيه رقم 95/46/ «إي سي» من البرلمان الأوروبي والمجلس الأوروبي في 24 أكتوبر 1995 عن حماية الأفراد فيما يخصّ التعامل مع البيانات الشخصيّة وحرية حركة تلك البيانات».

http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML

المجلس الأوروبي (أبريل 2014). «كتاب إرشادي عن القانون الأوروبي لحماية البيانات».
http://www.echr.coe.int/Documents/Handbook_data_protection_ENG.pdf

24. زاك ويتاكر (25 أبريل 2011). موقع «زد دي نت». مقال: «الملاذ الآمن: لماذا تحتاج بيانات «الاتحاد الأوروبي» إلى «أن تُحمى» من القانون الأميركي».

ZDNet,
http://www.zdnet.com/blog/igeneration/safe-harbor-why-eu-data-needs-protecting-from-us-law/8801

25. جاي ستانلي (أغسطس 2004). «الاتحاد الأميركي للحريّات المدنيّة». مقال: «المُركّب الرقابي- الصناعي».
American Civil Liberties Union,
https://www.aclu.org/sites/default/files/FilesPDFs/surveillance_report.pdf

26. دانا بريست ووليام إم. آركين (19 يوليو 2010). صحيفة واشنطن بوست. مقال: «عالم خفي، ينمو ليخرج عن السيطرة».
Washington Post,
http://projects.washingtonpost.com/top-secret-america/articles/a-hidden-world-growing-beyond-control

27. روبرت أوهارو جونيور، دانا بريست ومارجواري سنسر (10 يونيو 2013). صحيفة واشنطن بوست. «تسريبات «وكالة الأمن القومي» تظهر مدى اعتماد المؤسّسة الاستخباراتيّة على متعاقدين خارجيّين».
Washington Post,
http://www.washingtonpost.com/business/nsa-leaks-put-focus-onintelligence-apparatuss-reliance-on-outside-contractors/2013/06/10/e940c4ba-d20e-11e2-9f1a-1a7cdee20287_story.html

28. لا يبدو مرجّحاً أنه امتلك من أوقات الفراغ ما يكفي كي يبتكر أشياء قابلة للتطبيق مباشرة في وظيفته الجديدة. شاين هاريس (29 يونيو 2014). مجلة فورين بوليسي. مقال: «ملك الفضاء السبراني في «وكالة الأمن القومي»، يصبح شركة».
Foreign Policy,
http://www.foreignpolicy.com/articles/2014/07/29/the_crypto_king_of_the_NSA_goes_corporate_keith_alexander_patents.
كونور فيدرسدورف (31 يوليو 2014). مجلة آتلانتيك. مقال: «خطة كيث آلكسندر للغنى السريع ليست أخلاقيّة».
Atlantic,
http://www.theatlantic.com/politics/archive/2014/07/keith-alexandersunethical-get-rich-quick-plan/375367

29. سبنسر إكرمان (17 أكتوبر 2014)، صحيفة الغارديان، مقال: «مسؤول رفيع في «وكالة الأمن القومي» يضيء الطريق أمام شركة أمن خاصة».
Guardian,
http://www.theguardian.com/us-news/2014/oct/17/senior-nsa-official-moonlighting-private-cybersecurity-firm.

30. «إيلامان- غاما غروب» (2011). موقع «ويكيليكس». «الحلول الأمنيّة الألمانيّة».
Wikileaks,
https://s3.amazonaws.com/s3.documentcloud.org/documents/810435/313-elaman-product-list-finfisher.pdf.

31. مورغان ماركيز- بوار وبيل ماركزاك (29 أغسطس 2012). جامعة تورنتو، «مختبر المواطن»، «مركز مونك للدراسات الدوليّة». مقال: «الهاتف الذكي الذي أحبّني: «فِن- فيشر» ينتقل إلى الخلوي؟»
http://citizenlab.org/2012/08/the-smartphone-who-loved-me-finfisher-goes-mobile
نيكول بيلروث (30 أغسطس 2012)، صحيفة نيويورك تايمس. مقال: «برنامج كومبيوتر صمّم ليكافح الجريمة لكنه يستعمل للتجسّس على المنشقّين».
New York Times,
http://www.nytimes.com/2012/08/31/technology/finspy-software-is-tracking-political-dissidents.html.

32. بيـل ماركزاك وآخـرون (17 فبراير 2014). مقال: «رسـم تخطيطي لبرنامج كومبيوتر للتجسّـس من صنع «هاكينغ تيم». جامعة تورنتو، «مختبر المواطن»، «مركز مونك للدراسات الدوليّة».
https://citizenlab.org/2014/02/mapping-hacking-teams-untraceablespyware.

33. فيرنون سـيلفر وبن إلغين (22 أغسـطس 2011). شبكة «بلومبرغ نيوز». «التعذيب في البحرين يغدو روتينياً بمساعدة من'نوكيا' و'سيمنز'».
Bloomberg News,
http://www.bloomberg.com/news/2011-08-22/torture-in-bahrain-becomes-routine-with-help-from-nokia-siemens-networking.html.

34. مس سميث (10 نوفمبر 2011). مجلة نتورك وورلد. مقال: «مؤتمر التجسّس السري للحكومات: كنْ شبحيّاً، واضرب مئات آلاف الأهداف».
Network World,
http://www.networkworld.com/article/2221080/microsoft-subnet/secret-snoop-conference-for-gov-t-spying---go-stealth--hit-a-hundred-thousand-targe.html
جنيفر فالنتيو- ديفريز، جوليا آنغوين وستيف ستكلو (19 نوفمبر 2011). صحيفة وول ستريت جورنال. مقال: «كنز من الوثائق يكشف طرق الرقابة».
Wall Street Journal,
http://online.wsj.com/news/articles/SB10001424052970203611404577044192607407780.
Vernon Silver (21 Dec 2011), «Spies fail to escape spyware in $5 billion bazaar for cyber arms,» *Bloomberg News,*
http://www.bloomberg.com/news/2011-12-22/spies-fail-to-escape-spyware-in-5-billion-bazaarfor-cyber-arms.html.

35. تدريب في «عالم آي إس إس». (3-4 مارس 2014). دبي، الإمارات العربيّة.
http://www.issworldtraining.com/iss_mea/Brochure01.pdf

36. تملك «منظمة الشفافيّة الدوليّة» لائحة عمن حضروا تلك المؤتمرات بين عامي 2006 و2009.
Privacy International (2012), «Surveillance Who's Who,»
https://www.privacyinternational.org/sww

37. يـووي بيوز ومارسـيل روزنباخ (8 ديسـمبر 2011). صحيفة دير شـبيغيل. مقال: «عدو دولة الشـفافيّة: تكنولوجيا الرقابة الغربيّة في أيدي الطُغاة».
Der Spiegel,
http://www.spiegel.de/international/world/the-transparent-state-enemy-western-surveillance-technology-in-the-hands-of-despots-a-802317.html.

38. «فيجنغاين» (8 يناير 2013). وكالة «رويترز» للأنباء. «وفق تقرير «فيجنغاين»، قيمة سوق السلاح السبراني عالميّاً 16.9 بليون دولار في العام 2013».
Reuters,
http://www.reuters.com/article/2013/01/08/idUSnPre7f3zna+100+PRN20130108
جيمس بامفورد (12 يونيو 2013). مجلة وايرد. مقال: «الحرب السريّة».
Wired,
http://www.wired.com/2013/06/general-keith-alexander-cyberwar/all.

39. بول صون ومارغريت كوكر (30 أغسـطس 2011). صحيفة وول ستريت جورنال. مقال: «شركات ساعدت جواسيس ليبيّين».
Wall Street Journal,
http://online.wsj.com/news/articles/SB10001424053111904199404576538721260166388

40. «إلبايت سيسـتمز» (24 أبريل 2013). «نالت شركة «إلبايت سيسـتمز» عقداً بـ40 مليون دولار كي تمدّ دولة في أفريقيا بنظام «وايز انتليجانت تكنولوجيز».

http://ir.elbitsystems.com/phoenix.zhtml?c=61849&p=irolnewsArticle&ID=1810121.

41. صحيفة دير شبيغيل (11 أبريل 2012). مقال: «تعقّب المعارضة: مزاعم ببيع «سيمنز» نظاماً تقنياً للتعقب إلى سوريا».

Der Spiegel,
http://www.spiegel.de/international/business/ard-reports-siemens-sold-surveillance-technology-to-syria-a-826860.html.

42. بن إليغن وماريون سيلفر (3 نوفمبر 2011). شبكة «بلومبرغ نيوز». مقال: «القمع السوري يلقى معونة من شركة إيطاليّة وأداة أوروبيّة- أميركيّة للتجسّس».

Bloomberg News,
http://www.bloomberg.com/news/2011-11-03/syria-crackdown-gets-italy-firm-s-aid-withu-s-europe-spy-gear.html.

43. بول صون ومارغريت كوكر (30 أغسطس 2011). صحيفة وول ستريت جورنال. مقال: «شركات ساعدت جواسيس ليبيّين».

Wall Street Journal,
http://online.wsj.com/news/articles/SB10001424053111904199404576538721260166388

44. سارة كينزيور وكاتي بيرس (11 مايو 2012). موقع «سلايت». مقال: «كيف شيطنت الحكومة الأذربيجانيّة الإنترنت كي يبتعد المواطنون عنها».

Slate,
http://www.slate.com/blogs/future_tense/2012/05/11/azerbaijan_eurovision_song_contest_and_keeping_activists_and_citizens_off_the_internet_.html.

45. سارة كينزيور (يوليو 2012). «مؤسّسة أميركا الجديدة». بحث: «الحرية الرقميّة في التعبير عن الرأي في أوزبكستان: نموذج عن الحجب والسيطرة الاجتماعيّة».

46. «معهد التكنولوجيا المفتوحة». (9 ديسمبر 2013). وثيقة: «التوصل إلى اتفاقيّة دوليّة تمنع تصدير تكنولوجيا الرقابة المكثفة». «مؤسّسة أميركا الجديدة».

New America Foundation,
http://oti.newamerica.net/blogposts/2013/international_agreement_reached_controlling_export_of_mass_and_intrusive_surveillance

47. يووي بيوز ومارسيل روزنباخ (8 ديسمبر 2011). صحيفة دير شبيغيل. مقال: «عدو دولة الشفافيّة: تكنولوجيا الرقابة الغربيّة في أيدي الطُغاة».

Der Spiegel,
http://www.spiegel.de/international/world/the-transparent-state-enemy-western-surveillance-technology-in-the-hands-of-despots-a-802317.html.

48. القائمة الكاملة لتلك البلدان هي: أفغانستان، البحرين، بورما، الصين، مصر، الهند، أندونيسيا، العراق، كينيا، كويت، لبنان، ماليزيا، نيجيريا، قطر، روسيا، السعودية، سنغافورة، كوريا الجنوبيّة، سوريا، تايلاند، تركيا، فنزويلا. إيرين بواترانتو وفريقها (9 نوفمبر 2011). «وراء «بلو كوت»: تحقيقات عن الترشيح التجاري في سوريا وبورما». جامعة تورنتو، «مختبر المواطن»، «مركز مونك للدراسات الدوليّة».

https://citizenlab.org/2011/11/behind-blue-coat.

إيرين بواترانتو وفريقها (29 نوفمبر 2011). «وراء «بلو كوت»: متابعة عن بورما». جامعة تورنتو، «مختبر المواطن»، «مركز مونك للدراسات الدوليّة».

Citizen Lab, Munk School of Global Affairs, University of Toronto,
https://citizenlab.org/2011/11/behind-blue-coat-an-update-from-burma.

مورغان- ماركيز بوار وآخرون (24 يونيو 2014). جامعة تورنتو، «مختبر المواطن»، «مركز مونك للدراسات الدوليّة». مقال: «عالم «بلو كوت»: خريطة عالميّة لأدوات التتبع والرقابة».

Citizen Lab, Munk School of Global Affairs, University of Toronto,

https://citizenlab.org/2013/01/planet-blue-coat-mapping-global-censorshipand-surveillance-tools.

49. آدم سـنفت وآخرون (20 فبراير 2014). جامعة تورنتو، «مختبر المواطن»، «مركز مونك للدراسـات الدوليّة». مقال: «رقابة الإنترنت في دولة فاشلة: برنامج «نتسويبر» في الصومال».
https://citizenlab.org/2014/02/internet-filtering-failed-state-case-netsweeper-somalia

حلمي نعمان وآخرون. جامعة تورنتو، «مختبر المواطن»، «مركز مونك للدراسات الدوليّة». مقال: «يا باكستان نحن نراقبك: تحليل عن دور شركة «نتسويبر الكنديّة في نظام الحجب في باكستان».
Citizen Lab, Munk School of Global Affairs, University of Toronto,
https://citizenlab.org/2013/06/o-pakistan

50. مبادرة الشبكة المفتوحة (12 أكتوبر 2005). وثيقة: «رقابة الانترنت في بورما 2005».
https://opennet.net/sites/opennet.net/files/ONI_Burma_Country_ Study.pdf.

«ضوء جديد على ماينمار» (12 أكتوبر 2005). (16 مايو 2004). مقال: «رئيس الوزراء يحضر حفلاً لإدخال «جدار الوقاية من الفيروسات» الذي تصنعه «فورتينت»».
Firewall,» *New Light of Myanmar*,
http://www.myanmar.gov.mm/NLM-2004/May04/enlm/May16_h1.html

51. بـن أرنولدي (10 أكتوبر 2007). صحيفة كريسـتيان سـاينس مونيتور. مقـال: «عندما تصل «برمجيّات الرقابة» الأميركيّة إلى القبضات الإيرانيّة».
Christian Science Monitor,
http://www.csmonitor.com/2007/1010/p01s01-ussc.html.

52. مكتـب الأمم المتحـدة للمكافحة المخـدرات والجريمة. (سـبتمبر 2012). وثيقة: «اسـتعمال الإنترنت لأهداف إجراميّة».
http://www.unodc.org/documents/frontpage/Use_of_Internet_for_Terrorist_Purposes.pdf

53. موقع «بلانيت بيوميتركس» (2 مارس 2011). مقال: «التقنيّات البيومتريّة تنتشر في عالم ديزني».
http://www.planetbiometrics.com/article-details/i/504.

54. الكونغـرس الأميركـي (2012). وثيقة: «وزارة الخارجيّـة تعرب عن تقديرها للتحديثـات والتعديلات التقنيّة لقانون 2012». القانون العام 283.
http://www.gpo.gov/fdsys/pkg/PLAW-112publ283/html/PLAW-112publ283.htm

55. شارلي سافاج (7 مايو 2013). صحيفة نيويورك تايمس. مقال: «الولايات المتحدّة تقيّم عملية تجديد قوانين التنصّت».
New York Times,
http://www.nytimes.com/2013/05/08/us/politics/obama-may-back-fbi-plan-to-wiretap-web-users.html.

56. شـارلي سـافاج (27 سـبتمبر 2010). صحيفة نيويورك تايمس. مقـال: «الولايات المتحدة تحاول تسـهيل التنصّت على الإنترنت».
New York Times,
http://www.nytimes.com/2010/09/27/us/27wiretap.html

57. تيم روجرز (نوفمبر 2013). «القصة الحقيقيّة لمؤسّس «لافابِت».
D Magazine,
http://www.dmagazine.com/publications/d-magazine/2013/november/real-story-of-lavabit-founder-ladar-levison

58. سـبنسر إكرمان (9 أغسـطس 2013). صحيفـة الغارديان. مقال: «إغـلاق مفاجئ لخدمـة «لافابِت» للبريد الإلكتروني، مع الإشارة إلى تدخّل حكومي».
Guardian,
http://www.theguardian.com/technology/2013/aug/08/lavabit-e-mail-shut-downedward-snowden

لادار لِفيـزون (20 مايو 2014). صحيفة الغارديان. مقال: «أسرار وأكاذيب وبريد سـنودن الإلكتروني: لماذا اضطررت إلى إغلاق «لافابِت»».

Guardian,

http://www.theguardian.com/commentisfree/2014/may/20/why-did-lavabit-shut-down-snowden-email

59. ديكلان ماكولاغ (24 يوليو 2013). موقع «سي نِت». مقال: «الشرطة الفيدراليّة تضغط على شركات الـ«ويب» بهدف الحصول على المفاتيح الأساسيّة للتشفير».

CNET,

http://www.cnet.com/news/feds-put-heat-on-web-firms-for-master-encryption-keys

60. لِفيـزون هُـدّد بالاعتقـال لأنه أغلق «لافابِت» بأكثر من مسـألة السـماح للـ«إف بـي آي» بالنفاذ غير المشروط لحسـابات مسـتخدميها كافة. مايكل إيزيكوف (13 أغسطس 2013). شبكة «آن بي سي نيوز». مقال: «مالك شركة «لافابِت.كوم»: من الممكن اعتقالي بسبب مقاومة أمر بالرقابة».

NBC News,

http://www.nbcnews.com/news/other/lavabit-com-owner-i-could-be-arrested-resisting-surveillance-order-f6C10908072.

61. سيرج مالينكوفيتش (21 مارس 2013). نشرة كاسبارسكي دايلي. مقال: «هل يراقب «الأخ الكبير» حسابك على «سكايب»؟»

Kaspersky Lab Daily,

http://blog.kaspersky.com/skype-government-surveillance.

جيمـس ريزن وِنك وينغفيل (20 يونيو 2013). صحيفة نيويورك تايمس. مقال: «وكالة تجسّـس و«وادي السيليكون» تربطهما تقوية الإنترنت».

New York Times,

http://www.nytimes.com/2013/06/20/technology/silicon-valley-and-spy-agency-boundby-strengthening-web.html.

62. شركـة «مايكروسـوفت». (13 أكتوبر 2011). «مركز أخبار مايكروسـوفت». مقال: ««مايكروسـوفت» تضم «سكايب» رسمياً».

Microsoft News Center,

http://wwwmicrosoft.com/en-us/news/press/2011/oct11/10-13skypepr.aspx

63. غلـين غرينوالد (11 يوليو 2013). صحيفة الغارديان. مقال: «مايكروسـوفت سـلّمت «وكالة الأمن القومي» منفذاً إلى الرسائل المشفّرة».

Guardian,

http://www.theguardian.com/world/2013/jul/11/microsoft-nsa-collaboration-user-data

64. كريـغ تيمبرغ (11 سـبتمبر 201). صحيفة واشـنطن بوسـت. مقـال: «الحكومة الأميركيّـة هددت بفرض غرامات ضخمة ما لم يعطها «ياهوو» بياناته».

Washington Post,

http://www.washingtonpost.com/business/technology/us-threatened-massive-fine-toforce-yahoo-to-release-data/2014/09/11/38a7f69e-39e8-11e4-9c9f-ebb47272e40e_story.html.

65. جوزيف مِنن (20 ديسـمبر 2013). وكالة «رويترز» للأنباء. مقال: «عقد سري ربط «وكالة الأمن القومي» مع إحدى الشركات الرائدة في صناعة المعلوماتيّة».

Reuters,

http://www.reuters.com/article/2013/12/20/us-usa-security-rsa-idUSBRE9BJ1C220131220

66. المستوى 3 في الاتصالات يحمل الاسم الشيفري «ليتل». وبوجه عام، إذا كان مقدّم خدمة الإنترنت الذي تعتمده لديه اسم شيفري في الوكالة، فالأرجح أنك مكشوف. نيكول بيلروث (25 نوفمبر 2013). صحيفة **نيويورك تايمس**.
New York Times,
http://www.nytimes.com/2013/11/26/technology/a-peephole-for-the-nsa.html

67. براندون داوني (30 أكتوبر 2013). موقع «غوغل+». «إنها القصة الكبرى في عالم المعلوماتيّة الآن».
Google Plus,
https://plus.google.com/+BrandonDowney/posts/SfYy8xbDWGG

68. رايان غالاهار وغلين غرينوالد (12 مارس 2014). موقع «إنترسبت». «خطة «وكالة الأمن القومي» لنشر برمجيّات خبيثة في ملايين الحواسيب».
Intercept,
https://firstlook.org/theintercept/article/2014/03/12/nsa-plans-infect-millions-computers-malware.

69. شون غالاهار (14 مايو 2014). موقع «آرس تكنيكا». مقال: «صور مصنع «الترقية» لـ«وكالة الأمن القومي» تظهر زرع مكوّنات في محوّلات شركة «سيسكو».
http://arstechnica.com/tech-policy/2014/05/photos-of-an-nsa-upgrade-factory-show-ciscorouter-getting-implant

سارة سيلبرت (16 مايو 2014). مقال: «وثيقة حديثة من سنودن تظهر أن «وكالة الأمن القومي» اعترضت محوّلات «سيسكو» ودست مكوّنات فيها».
http://www.engadget.com/2014/05/16/nsa-bugged-cisco-routers.

جيمس بول وجوليان بورغر وغلين غرينوالد (5 سبتمبر 2013). صحيفة **الغارديان**. مقال: «كشف أخيراً: تآزر وكالات التجسّس الأميركيّة والبريطانيّة في هزيمة الخصوصيّة والأمن على الإنترنت».
Guardian,
http://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security

نيكول بلروث وجيف لارسون وسكوت شاين (5 سبتمبر 2013). صحيفة **نيويورك تايمس**. مقال: «تمكّن «وكالة الأمن القومي» من الإطاحة بأساسيّات حماية الخصوصيّة على الـ«ويب»».
New York Times,
http://www.nytimes.com/2013/09/06/us/nsa-foils-much-internet-encryption.html

70. برايان كريبس (28 مايو 2014). ««باب خلفي» في معدّات رصد المكالمات، هو أداة رقابة».
Krebs on Security,
http://krebsonsecurity.com/2014/05/backdoor-in-call-monitoring-surveillance-gear

71. بيتر مآس ولورا بواتراس (10 أكتوبر 2014). موقع «إنترسبت». مقال: «سّر كبير: تملك «وكالة الأمن القومي» مخرّبين يعملون في ألمانيا والصين».
Intercept,
https://firstlook.org/theintercept/2014/10/10/core-secrets

72. مارتن برابنت (7 مارس 2014). موقع «نكست ويب». مقال: ««غوغل» مطمئن «إلى حدّ كبير» أن البيانات باتت الآن بمنأى عن العيون الحكومية المتفحصة، وفق إريك شميدت».
Next Web,
http://thenextweb.com/google/2014/03/07/google-pretty-sure-protected-government-spying-eric-schmidt-says

الفصل 7: العدالة والحريّة السياسيّة

1. ديفيد غرين (27 يناير 2014). «مؤسّسة الحدود الإلكترونيّة». مقال: «غوص في قضيّة الكنيسة التوحيديّة ضد «وكالة الأمن القومي»: عن أهميّة الحق في إنشاء روابط».

Electronic Frontier Foundation,
https://www.eff.org/deeplinks/2014/01/deep-divefirst-unitarian-church-v-nsa-why-freedom-association-matters

2. جوشوا إيتون (15 أغسطس 2014). موقع «يو يو ورلد». مقال: «تحدّي دولة الرقابة».

UU World,
http://www.uuworld.org/ideas/articles/297088.shtml

3. يوشاي بنكلر (13 سبتمبر 2013). صحيفة الغارديان. «حان الوقت للوقوف بوجه التلاعب الوحشي لـ«وكالة الأمن القومي» بحقوقنا».

Guardian,
http://www.theguardian.com/commentisfree/2013/sep/13/nsa-behemoth-trampling-rights.

4. مجلة الإيكونومست (16 نوفمبر 2013). مقال: «العالم المُسَجَّل: كل خطوة تخطوها».

Economist,
http://www.economist.com/news/leaders/21589862-cameras-become-ubiquitous-and-able-identify-people-more-safeguards-privacy-will-be

5. هارفي سيلفرغليت وتيم لينش (يناير/فبراير 2010). تقرير «معهد كاتو للسياسة». «تجريم الأشياء كلها تقريباً».

Cato Policy Report,
http://www.cato.org/policy-report/januaryfebruary-2010/criminalization-almost-everything.

هارفي سيلفرغليت (2011). كتاب ثلاث جنايات يوميّاً: عن استهداف ضباط الشرطة للأبرياء. دار «إينكاونتر» للكتب.

http://www.threefeloniesaday.com.

G. H. Reynolds (8 Jul 2013), «Ham sandwich nation: Due process when everything is a crime,»
Columbia Law Review 113,
http://columbialawreview.org/ham-sandwich-nation_reynolds

6. روز سيوتا (4 مايو 2003). صحيفة فيلادلفيا إنكوايرر. مقال: «نقّاد يرصدون توسّعاً في قوانين الدليل المادي».
Inquirer,
http://articles.philly.com/2003-05-04/news/25460033_1_material-witness-law-material-witnesses-material-witness-statute

آنيا مالهوترا (27 يونيو 2005). منظمة «هيومن رايتس ووتش». «شاهد على إساءة الاستخدام: الإساءة إلى حقوق الإنسان في قانون الدليل المادي، منذ 11 سبتمبر».

Anjana Malhotra (27 Jun 2005), «Witness to abuse: Human rights abuses under the Material Witness Law since September 11,» Human Rights Watch,
http://www.hrw.org/sites/default/files/reports/us0605_0.pdf.

Naureen Shah et al.(21 Jul 2014), «Illusion of justice: Human rights abuses in US terrorism prosecutions,»Human Rights Watch,
http://www.hrw.org/node/126101

7. في ولاية «كارولينا الشماليّة» تعدُّ بندقيّة الصيد المقصوصة الماسورة سلاحاً للدمار الشامل. جوناثان ليمير (30 أغسطس 2011). صحيفة نيويورك ديلي تايمس. مقال: «إدانة طالب في «كارولينا الشماليّة» لأنه تباهى بامتلاك بندقيّة صيد مقصوصة الماسورة».

http://www.nydailynews.com/news/national/northcarolina-student-charged-weapon-mass-destruction-toting-sawed-off-shotgunarticle-1.950971

8. لويس جاكوبسون (9 يوليو 2013). موقع «بوليتي فاكت». مقال: «ما هو تعريف الـ«إرهاب»؟»
Politifact,
http://www.politifact.com/truth-o-meter/article/2013/jul/09/whats-definition-terrorism

9. دانيـال ج. سـولوف (2004). كتاب **الإنسـان الرقمـي: التكنولوجيا والخصوصيـة في عصر المعلومات.** «مطبعة جامعة نيويورك».
http://docs.law.gwu.edu/facweb/dsolove/Digital-Person/text/Digital-Person-CH3.pdf

10. اعتادت «وزارة الأمن الوطني»- وربما ما زالت- أن تراقب الشـبكات الاجتماعيّة كي تراقب ردود أفعال الناس على أخبار «مسـيئة للولايات المتحدة». إلين ناكاشـيما (13 يناير 2012)، صحيفة **واشـنطن بوسـت**. مقال: «يخشى نشطاء الحريّات المدنيّة من مراقبة «وزارة الأمن الوطني» للشبكات الاجتماعيّة».
Washington Post,
http://www.washingtonpost.com/world/national-security/dhs-monitoring-of-social-mediaworries-civil-liberties-advocates/2012/01/13/gIQANPO7wP_story.html.

11. هيئـة الإذاعة البريطانيّـة (31 يناير 2012). مقـال: «يُنصَح بتوخي الحذر على «تويتر»، بعد منع سـوّاح من دخول أميركا».
BBC News,
http://www.bbc.co.uk/news/technology-16810312

12. غيري سـميث (25 يونيـو 2014). صحيفة **هافنغتون بوسـت**. «كيف يقرأ البوليس «تويـتر» كله بحثاً عن مخاطر إرهابيّة».
Huffington Post,
http://www.huffingtonpost.com/2014/06/25/dataminr-mines-twitter-to_n_5507616.html.

13. فيليب ميسـنغ (13 أبريل 2013). صحيفة **نيويورك بوسـت**. مقال: «اعتقال راكب في مطار «جي أف كيه» لتحدّثه عن سندويتش «قنبلة»».
New York Post,
http://nypost.com/2013/04/13/jfk-passenger-detained-after-talking-about-bomb-sandwich

14. هناك مقال ممتاز عن ذلك الموضوع.
براكسـيس (17 ينايـر 2014). موقـع «ميديوم». مقـال: «العالم كله أصبـح الآن مطاراً: الرقابة والسـيطرة الاجتماعيّة».
Medium,
https://medium.com/i-m-h-o/9a1e5268ff39.

15. لورين راسـل (24 أبريل 2013). شـبكة «سي آن آن». مقال: «عندما يؤدّي الإفراط في مشـاركة المحتوى على الإنترنت إلى اعتقالك».
CNN,
http://www.cnn.com/2013/04/18/tech/social-media/online-oversharing-arrests

16. «هيئـة الإذاعـة البريطانيّة» (27 مارس 2012). مقال: «فابريس مواميا: مغرّد عنصري على «تويتر»، يسـجن لـ56 يوماً».
BBC News,
http://www.bbc.co.uk/news/uk-wales-17515992.

17. «هيئة الإذاعة البريطانيّة». (4 يونيو 2014). مقال: «رجل يسـجن بسـبب تدوينة على «فيسبوك» عدّت مسيئة لآن ماغواير».
BBC News,

http://www.bbc.co.uk/news/uk-england-27696446

18. جيرمي سـكاهيل وغلين غرينوالد (10 فبراير 2014). موقع «إنترسـبت». مقال: «الدور السري لـ«وكالة الأمن القومي» في برنامج الاغتيال الأميركي».

Intercept,
https://firstlook.org/theintercept/article/2014/02/10/the-nsas-secret-role

كوري كريدر (4 مارس 2014). قناة «الجزيرة» التلفزيونيّة. مقال: «القتل باسم الخوارزميّات».

Al Jazeera,
http://america.aljazeera.com/opinions/2014/3/drones-big-data-waronterrorobama.html

19. جون كاغ وسارة كريبس (2014). كتاب: أسلحة حرب الـ «درون». دار «ويلي» للنشر.

http://books.google.com/books?id=I8oOBAAAQBAJ.

20. ريتشـارد إنغل وروبرت ويندريم (5 يونيو 2013). شـبكة «آن بي سي نيوز». مقال: «وثائق تظهِر أن الـ«سي آي إيه» لم تكن تعرف نصف من قتلتهم بغارات الـ«درون»».

NBC News,
http://investigations.nbcnews.com/_news/2013/06/05/18781930-ciadidnt-always-know-who-it-was-killing-in-drone-strikes-classified-documents-show.

21. كارين ماكفيه (27 أغسـطس 2013). صحيفة الغارديان. مقـال: «وفق «الاتحاد الأميركي للحريّات المدنيّة»، يخالف برنامج رقابة الـ«وكالة الأمن القومي» الدستور».

Guardian,
http://www.theguardian.com/world/2013/aug/27/nsa-surveillance-program-illegal-aclu-lawsuit

22. أوليفـر أوغسـت (23 أكتوبر 2007). مجلة وايرد. «جـدار النار العظيم»: محاولة الصـين المتخبّطة والعبثيّة للسيطرة على ما يحدث على الـ«ويب»».

Wired,
http://www.oliveraugust.com/journalism_chinas-internet-heroes.htm.

23. غاري كينغ وجنيفر بان ومارغريت ي. روبرتس. (مايو 2013). مجلة أميركان بوليتيكال سـاينس ريفيو. مقال: «كيف يعمل الحجب في الصين على إثارة الانتقاد ضد الحكومة، لكنه يخرِس حرية التعبير الجماعيّة».

American Political Science Review 107,
http://gking.harvard.edu/publications/how-censorship-china-allows-government-criticism-silences-collectiveexpression

24. سـايتلن ديوي (12 أغسـطس 2013). صحيفة واشنطن بوسـت. مقال: «تقف «ويكيبيديا» شبه وحيدة في مواجهة طلبات صينيّة بممارسة رقابة ذاتيّة».

Washington Post,
http://www.washingtonpost.com/blogs/worldviews/wp/2013/08/12/wikipedia-largelyalone-in-defying-chinese-self-censorship-demands

25. رونالد دايبرت وآخرون (2010). كتاب: النفاذ تحت السـيطرة: رسـم شكل السلطة والحقوق والدور في الفضاء السبراني. (مطبعة «معهد ماساشوستس للتقنيّة»).

MIT Press,
http://mitpress.mit.edu/books/access-controlled.

26. مجلة فوربس. (25 ديسمبر 2000). مقال: «سوازتيكا. كوم».

Forbes,
http://www.forbes.com/forbes/2000/1225/6616164s1.html

27. «هيئة الإذاعة البريطانيّة» (1 سبتمبر 2013). مقال: «تفعيل القيود على الإنترنت في فيتنام».

BBC News,
http://www.bbc.com/news/world-asia-23920541.

28. رونالد دايبرت وآخرون (2010). كتاب: النفاذ تحت السيطرة: رسم شكل السلطة والحقوق والدور في الفضاء السبراني. (مطبعة «معهد ماساشوستس للتقنيّة»).

MIT Press,
http://mitpress.mit.edu/books/access-controlled

29. بن كوين (10 أكتوبر 2011). صحيفة الغارديان. مقال: «الشركات الأربع الأربعة الكبرى لتقديم خدمة الإنترنت في بريطانيا، تنتقل إلى «خيار عدم الخروج من الرقابة» بالنسبة للجنس الإباحي».
Guardian,
http://www.theguardian.com/society/2011/oct/11/pornography-internet-service-providers

أنطوني فيولا (28 سبتمبر 2013). صحيفة واشنطن بوست. مقال: «الإجراءات البريطانيّة الصارمة في الرقابة شبكيّاً لمواد الجنس الإباحي، تثير نقاشات عن حريّة التعبير».
Washington Post,
http://www.washingtonpost.com/world/europe/britainsharsh-crackdown-on-internet-porn-prompts-free-speech-debate/2013/09/28/d1f5caf8-2781-11e3-9372-92606241ae9c_story.html.

30. إيوين ماكآسكل (1 ديسمبر 2010). صحيفة الغارديان. مقال: «ضغوط سياسيّة تؤدي إلى سحب موقع «ويكيليكس» من «آمازون. كوم».
Guardian,
http://www.theguardian.com/media/2010/dec/01/wikileaks-website-cables-servers-amazon.

31. نيل ماكفاركوهار (6 مايو 2014). صحيفة نيويورك تايمس. مقال: «بهدوء، روسيا تشدّد قوانين الإنترنت بفرضها «قانون البلوغرز»».
New York Times,
http://www.nytimes.com/2014/05/07/world/europe/russia-quietly-tightens-reins-on-web-with-bloggers-law.html

32. يؤدّي جعل المواطن مخبراً إلى تسميم المجتمع، إذ يخلق رعباً واسعاً يوصل إلى تفكيك الأواصر الاجتماعيّة التي تربط الناس بعضها بعضاً. بروس شناير (26 أبريل 2007). مدوّنة إلكترونيّة. مقال: «في التمييز بين المخبر «الكريه» والمخبر المواطن».
Schneier on Security,
https://www.schneier.com/blog/archives/2007/04/recognizing_hin_1.html

33. جاسون كيو نغ (12 مارس 2012). موقع «وايجنغ نون فايولانس». مقال: «كيف جعلت الصين الإنترنت تراقب نفسها بنفسها؟»
Waging Nonviolence,
http://wagingnonviolence.org/feature/how-china-gets-the-internet-to-censor-itself

34. كويمنغ بانغ (2008). مجلة دراسات الاتّصال العالمي. دراسة: «الحجب الذاتي وصعود الجماعيّة على الإنترنت: دراسة أنثروبولوجيّة لمجتمع الصين الافتراضي».
http://www.uri.edu/iaics/content/2008v17n3/05%20Cuiming%20Pang.pdf.

35. جورج ل. وايت وفيليب ج. زيمباردو (مايو 1975). «مكتب البحريّة الأميركيّة للبحوث». دراسة: «التأثيرات المجمّدة للرقابة: نزع الفرديّة والتفاعل».
Office of Naval Research/National Technical Information Service,
http://www.dtic.mil/dtic/tr/fulltext/u2/a013230.pdf.

36. «المحكمة العليا الأميركيّة» (23 يناير 2012). قرار عن «الولايات المتحدة ضد جونز».
http://caselaw.lp.findlaw.com/scripts/getcase.pl?court=US&navby=case&vol=000&invol=10-1259#opinion1.

37. إيين موغلن (27 مايو 2014). صحيفة الغارديان. مقال: «الخصوصيّة تتعرّض للهجوم: وثائق «وكالة الأمن القومي» تكشف تهديدات جديدة للديمقراطيّة».
Guardian,

http://www.theguardian.com/technology/2014/may/27/-sp-privacy-under-attack-nsa-files-revealed-new-threatsdemocracy.

38. ج. آليكس سنها (28 يوليو 2014). مؤسّسة «هيومن رايتس ووتش». مقال: «لديهم حريّة أن يراقبوا الجميع».
Human Rights Watch,
http://www.hrw.org/reports/2014/07/28/libertymonitor-all.

39. في العـام 2014، علمنا أنّ «المديريّة الأسـترالية للإشـارات»، وهي الصنو الأسـترالي لـ«وكالـة الأمن القومي»، تنصّتت على الاتّصالات بين شركة «ماير براون» الأميركيّة للاستشـارات القانونيّة وزبونتها المتمثّلة في الحكومة الأندونيسـيّة. وأعطت المديريّة الأسـتراليّة تلـك البيانات إلى الوكالة. جيمس رايزن ولـورا بواتراس (15 فبراير 2014). صحيفـة **نيويـورك تايمس**. مقال: «تجسّـس شريـك لـ«وكالة الأمن القومي» شـمل شركة أميركيّة للاستشارات القانونيّة».

New York Times,
http://www.nytimes.com/2014/02/16/us/eavesdropping-ensnared-american-law-firm.html

40. ج. آليكس سنها (28 يوليو 2014). مؤسّسة «هيومن رايتس ووتش». مقال: «لديهم حريّة أن يراقبوا الجميع».
Human Rights Watch,
http://www.hrw.org/reports/2014/07/28/libertymonitor-all.

41. رابطة «بين أميركا» (2013). «تأثيرات مفزعة: رقابة «وكالة الأمن القومي» تدفع الكتّاب إلى الحجب الذاتي».
http://www.pen.org/sites/default/files/Chilling%20Effects_PEN%20American.pdf.

42. جـرى الاسـتطلاع مباشرة عقب ظهور الأخبـار الأولى عن جمع «وكالة الأمن القومـي» للـ«ميتاداتا» من شركة «فريـزون»، وافتراضاً من كل شـخص آخر؛ وحصولها على بيانات الإنترنت مـن شركات كـ«غوغل» و«ياهوو» و«فيسـبوك» و«مايكروسـوفت» و«تويتر». إليزابيث دويسكن (26 أغسـطس 2014). صحيفة **وول ستريت جورنال**. مقال: «استطلاع: الناس لا يتحدثون عن «وكالة الأمن القومي» على الإنترنت».
Wall Street Journal,
http://blogs.wsj.com/digits/2014/08/26/survey-people-dont-want-to-talk-online-about-the-nsa

43. آمريتـا جاياكومـار (2 أبريل 2014). صحيفة **واشـنطن بوسـت**. مقـال: «أميركيّون يقولـون إنهم صاروا يتسوّقون أقل على الإنترنت. الملامة تقع على «وكالة الأمن القومي»».

Washington Post,
http://www.washingtonpost.com/blogs/the-switch/wp/2014/04/02/americans-say-theyre-shopping-less-online-blame-the-nsa

44. داويـنـدر س. سـيدهو (2007). «التأثـير المفـزع لرقابـة الحكومـة في اسـتخدام الإنترنت من قِبَل المسـلمين الأميركيّين».
University of Maryland Law Journal of Race, Religion, Gender and Class 7,
http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1002145

45. ديفيد غرين (6 نوفمبر 2013). «مؤسّسة الحقوق الإلكترونيّة». مقال: «ملفات «مؤسّسة الحقوق الإلكترونيّة»: 22 شهادة مباشرة عن الفزع الذي أثارته رقابة «وكالة الأمن القومي»، بشأن الحق في الترابط».
https://www.eff.org/press/releases/eff-files-22-firsthand-accounts-hownsa-surveillance-chilled-right-association

46. آليكـس مارثـوز وكاثريـن توكر (24 مـارس 2014). «شـبكة بحوث علـم الاجتماع». ورقة بحـث: «الرقابة الحكوميّة وسلوك البحث على الإنترنت».

Social Science Research Network,
http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2412564

47. «المفوضيّة العليا لحقوق الإنسان في الأمم المتّحدة» (30 يونيو 2014). «العصر الرقمي والحق في الخصوصيّة».
http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session27/Documents/A.HRC.27.37_en.pdf.

48. ليز كلايمز (22 مارس 2012). موقع «بلايز». مقال: «مجرّد زيارة موقع شبكي لإرهابيّين تؤدي إلى السجن في فرنسا».
Blaze,
http://www.theblaze.com/stories/2012/03/22/simply-visiting-terrorist-websites-could-mean-jail-time-infrance.

49. راشيل كلارك (11 يوليو 2013). مقال: «كل شيء عن كل شخص: عمق رقابة الـدستازي» في «جمهورية ألمانيا الديمقراطيّة»».
http://thevieweast.wordpress.com/2013/07/11/everything-about-everyone-the-depth-of-stasi-surveillance-inthe-gdr.

أوكا إيفاجين (20 أغسطس 2014). مقال: «مكالماتكم الهاتفيّة ستراقب قريباً».
http://pulse.ng/lifestyle/tech/security-vs-privacy-your-calls-may-soon-be-monitored-ncc-id3066105.html.

50. كارل غواشيم فريدريتش (أكتوبر 1939). «الديمقراطيّة والتمرّد».
Political Quarterly 10,
http://onlinelibrary.wiley.com/doi/10.1111/j.1467-923X.1939.tb00987.x/abstract.

51. بروس شناير (2012). كتاب: **كَذَبَة ومتمردون: تفعيل الثقة التي يحتاجها المجتمع لينمو**. دار «ويلي» للنشر.
http://www.wiley.com/WileyCDA/WileyTitle/productCd-1118143302.html.

52. فرانك زابا وبيتر أوشيوكروسّو (1989). كتاب: **كتاب فرانك زابا الحقيقي**. دار «بوزيدون برس».
http://books.google.com/books?id=FB0O_HCpBy0C.

53. يشدّد أستاذ القانون في «جامعة واشنطن» البروفسور نيل ريتشاردز على تلك الفكرة بالقول: «تتطوّر الأفكار الجديدة بأفضل الطُرُق، عندما تكون بعيدة عن التدقيق المتمحّص للانكشاف العمومي». نيل ريتشاردز (مايو 2013) بحث: «مخاطر الرقابة».
Harvard Law Review 126,
http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2239412

54. تستخدم السلطات المحليّة في مدينة «بلتيمور» الصور الجويّة في ملاحظة مخالفات البناء، إذ تقارنها مع قاعدة بياناتها عن رخص البناء. دوو دونوفان (7 سبتمبر 2004). صحيفة **بلتيمور صن**. مقال: «نظرة من فوق لكل مبنى في المدينة».
Baltimore Sun,
http://articles.baltimoresun.com/2004-09-07/news/0409070310_1_images-deck-aerial

55. غريغوري كونتي (4 ابريل 2014). «نظرية للبقاء بالنسبة للحوكمة والإنفاذ المؤتمت للقانون».
http://robots.law.miami.edu/2014/wp-content/uploads/2013/06/Shay-etal-TheoryofConservation_final.pdf.

56. يصلح نموذجاً على ذلك «الشرطي آكل لحوم البشر» الذي دردش في الإنترنت مع أصدقائه، عن اغتصاب زوجته والتهامها مع أخريات؛ لكنه لم يفعل شيئاً. دانيال بيكمان وداريه غريغوريان (1 يوليو 2014). صحيفة **نيويورك تايمس**. مقال: «إطلاق سراح» الشرطة آكل لحوم البشر»، بعد أن انقلبت أمور التهمة بشكل مذهل».
New York Daily News,
http://www.nydailynews.com/new-york/nyc-crime/conviction-cannibal-nypd-overturned-article-1.1850334.
Daniel Engber (2 Jul 2014), «The cannibal cop goes free, but what about the murderous mechanic?»
Slate,
http://www.slate.com/articles/news_and_politics/crime/2014/07/the_cannibal_cop_gilberto_valle_goes_free_what_about_michael_van_hise_and.html.

57. والـتر بيري وآخرون (2013). «مؤسّسـة راند». بحث: «شرطـة توقّعيّة: دور توقّع الجرائـم في عمليات إنفاذ القانون».

RAND Corporation,
https://www.ncjrs.gov/pdffiles1/nij/grants/243830.pdf.

58. مايـكل ل. ريتـش (مارس 2013). مجلـة هارفرد للقانون والسياسـة العامة. بحـث: «أيجب علينا جعل الجريمة مستحيلة».

Harvard Journal of Law and Public Policy 36,
http://www.harvard-jlpp.com/wp-content/uploads/2013/04/36_2_795_Rich.pdf

59. يوشـاي بِنكلر (4 ديسـمبر 2013) «مركز بحوث جامعة هارفرد عن الحوسـبة والمجتمع». بحث: «النظام والضمير: الرقابة الواسعة لـ«وكالة الأمن القومي» ومسألة الحريّة».

Center for Research on Computation and Society, Harvard University,
http://crcs.seas.harvard.edu/event/yochai-benklercrcs-lunch-seminar
and
https://www.youtube.com/watch?v=6EUueRpCzpw

60. وليام ي. كولبي (1976). مجلة الأمن الدولي. مقال: «الأمن وسريّة الاستخبارات في المجتمع الحرّ».
International Security 1,
http://people.exeter.ac.uk/mm394/Intelligence%20Secrecy%20and%20Security.pdf
جيمس ي. نوت (صيف 1975). مقال: «السريّة والاستخبارات في مجتمع حرّ».
Studies in Intelligence 19,
https://www.cia.gov/library/centerfor-the-study-of-intelligence/kent-csi/vol19no2/html/v19i2a01p_0001.htm

61. باميلا و. لونغ وآليكس رولاند (1994). بحث: «السريّة العسكريّة في الماضي وفي أوروبا القرون الوسطى: تقييم نقدي». مجلة هستوري أند تكنولوجي.

History and Technology 11,
http://www.tandfonline.com/doi/abs/10.1080/07341519408581866?journalCode=ghat20

62. لويس أ. كوزر (صيف 1963). مقال: «اختلالات وظيفيّة في السريّة العسكريّة». مجلة سوشال بروبلمز.
Social Problems 11,
http://www.jstor.org/discover/10.2307/798801

63. 613 كان المثـال الأبـرز على ذلك هو السريّة والخـداع اللذان أحاطا بعملية إنزال قوات الحلفاء على شـواطئ النورماندي. جون س. ويندل (1997). سـلاح الجو الأميركي. تقرير: «عملية الخداع الاستراتيجي التي رافقت غزو النورماندي».

http://www.globalsecurity.org/military/library/report/1997/Wendell.htm
دان لاموث (6 يونيو 2014). صحيفة واشـنطن بوسـت. مقال: «ذكرى الأكاذيب والسريّة العسـكريّة التي أنجَحَتْ الإنزال على النورماندي».

Washington Post,
http://www.washingtonpost.com/news/checkpoint/wp/2014/06/06/remembering-the-military-secrecy-and-liesthat-made-d-day-successful.

64. سـيفن آفترغود (أكتوبر 1999). «مركز جامعة كورنيل لدراسـات السـلام». ورقة بحـث: «السريّة الحكوميّة وإنتاج المعرفة: مسح إحصائي عن بعض القضايا العامة».

http://large.stanford.edu/publications/crime/references/dennis/occasional-paper23.pdf.
Francis B. Kapper (Oct 1999), «The role of government in the production and control of scientific and technical knowledge,» ibid
كوين فارمر ودانيال ماغروسكي (يونيو 2012). مجلة بريتش جورنال أوف هستوري أوف ساينس. ورقة بحث: «ولايات السريّة: مدخل».

British Journal of the History of Science 45,
http://journals.cambridge.org/action/displayAbstract?fromPage=online&aid=8608487&fileId=S0007087412000052

65. بيتر غاليسون (خريف 2004)، «كريتيكال إنكوايري». مقال: «إزالة المعرفة».
Critical Inquiry 31,
http://www.fas.harvard.edu/~hsdept/bios/docs/Removing%20Knowledge.pdf.

66. المرجع السابق.

67. «المكتب الأميركي للإدارة والموازنة» (فبراير 2014). تقرير: «مراجعة العمليات الأمنيّة ومدى تناسبيّتها».
http://www.fas.org/sgp/othergov/omb/suitsec-2014.pdf.

68. وفق كلايبر، وهو مدير الاستخبارات القوميّة: «الكشف عن المعلومات تكون سريّة وتتّصل بالتفاصيل العملية لـ«وكالة الأمن القومي» وأمديتها، وفق ما ورد في تلميحات المدّعين؛ من شأنه أن يتسبّب بضرر بالغ للأمن القومي للولايات المتحدة».
جيمس ر. كلايبر (20 ديسمبر 2013). «إعلان عام من جيمس ر. كلايبر، مدير الاستخبارات القوميّة».
Jewel et al. v. National Security Agency et al. (08-cv-4873-JSW; *Shubert, et al., v. Obama, et al.* (07-cv-693-JSW), United States District Court for the Northern District of California,
http://www.dni.gov/files/documents/1220/DNI%20Clapper%202013%20Jewel%20Shubert%20SSP%20Unclassified%20Signed%20Declaration.pdf

69. بعد كشوفات سنودن، رفعت محكمة «فيسا» غطاء السريّة عن معظم أحكامها العامة. ولم يكن ليحصل ذلك الأمر أيضاً لو لم يفعل سنودن ما فعله.

70. جنيفر فالنتينو- دي فرايز (2 يونيو 2014). صحيفة وول ستريت جورنال. مقال: «ملفات مقفلة لإحدى المحاكم، عن المساعدة في تمويه الرقابة الإلكترونيّة».
Wall Street Journal,
http://online.wsj.com/news/article_email/sealed-court-files-obscure-rise-in-electronic-surveillance-1401761770-lMyQjAxMTA0MDAwMzEwNDMyWj

71. جوزيف كوكس (7 أغسطس 2014). موقع «فايس». مقال: «لا تعترف الشرطة البريطانية أنّه يتتبّع المكالمات الهاتفيّة للناس».
Vice,
http://motherboard.vice.com/read/uk-police-wont-admit-theyre-tracking-peoples-phone-calls

72. ثمة قصة عن المعايشة المباشرة لتجربة تلقي ذلك النوع من رسائل «وكالة الأمن القومي». في البداية، نُشرت تلك القصة باعتبارها من مجهول، ثم تبيّن أنها لبروستر كاهيل، مؤسّس «أرشيف الإنترنت». مجهول (23 مايو 2007). صحيفة واشنطن بوست. مقال: «رسالة إليّ من الأمن القومي، مع أمر قضائي بالصمت».
http://www.washingtonpost.com/wp-dyn/content/article/2007/03/22/AR2007032201882.html

73. 623 كيم زتر (3 مارس 2014). مجلة وايرد. مقال: «سلاح سري لشرطة فلوريدا: تتبع الهواتف من دون مذكرات قضائيّة».
Wired,
http://www.wired.com/2014/03/stingray
كيم زتر (4 مارس 2014). مجلة وايرد. مقال: «عقدت الشرطة مع صانع محلي لأداة تتبع، يمنع الحديث عن تلك الأداة».
Wired,
http://www.wired.com/2014/03/harris-stingray-nda

74. داروين بوند- غراهام وآلي ونستون (30 أكتوبر 2013). مجلة سان فرانسيسكو ويكلي. مقال: «كل جرائم الغد: مستقبل الشرطة يبدو أقرب إلى التصنيف في ماركات تجاريّة».
SFWeekly,

http://www.sfweekly.com/2013-10-30/news/predpol-sfpd-predictive-policingcompstat-lapd/full.

75. جنيفر ك. إليسا (10 يناير 2013). بحث: «حماية المعلومات السريّة: الإطار القانوني».
Congressional Research Service,
http://fas.org/sgp/crs/secrecy/RS21900.pdf.

76. كاري نيوتن ليون (2007). «لويس أند كلارك لو ريفيو». تقرير: «حظوة أسرار الدولة: توسّع مداها مع إساءة الحكومة استخدام السلطة».
Lewis and Clark Law Review 99,
http://www.fas.org/sgp/jud/statesec/lyons
سودها سيتي (يوليو 2012). مجلة كونكتيكت لو ريفيو. مقال: «صعود أسرار الأمن القومي».
Connecticut Law Review 44,
http://connecticutlawreview.org/files/2012/09/5.Setty-FINAL.pdf

77. إريك ليشتبلاو وسكوت شاين (9 يوليو 2006). صحيفة نيويورك تايمس. مقال: «أحد الحلفاء نصح بوش بإبقاء التجسّس بعيداً عن الكونغرس».
New York Times,
http://www.nytimes.com/2006/07/09/washington/09hoekstra.html
سكوت شاين (11 يوليو 2009). صحيفة نيويورك تايمس. مقال: «صلة شيني بإخفاء مشروع للـ«سي آي إيه»».
New York Times,
http://www.nytimes.com/2009/07/12/us/politics/12intel.html.
بول لويس (31 يوليو 2013). صحيفة الغارديان. مقال: «البيت الأبيض يعجز عن تأكيد إبلاغه الكونغرس عن برنامج «وكالة الأمن القومي» في التجسّس».
Guardian,
http://www.theguardian.com/world/2013/jul/31/white-house-congress-nsa-xkeyscore

78. بارتون غيلمان (15 أغسطس 2013). صحيفة واشنطن بوست. مقال: «ما نقول، وما لا نقول؛ لمن «يشرفون» علينا».
Washington Post,
http://apps.washingtonpost.com/g/page/national/what-to-say-and-not-to-say-to-our-overseers/390.

79. غلين غرينوالد (4 أغسطس 2013). صحيفة الغارديان. مقال: «أعضاء في الكونغرس يُمنعون من معلومات أساسيّة عن «وكالة الأمن القومي»».
Guardian,
http://www.theguardian.com/commentisfree/2013/aug/04/congress-nsa-denied-access

80. سبنسر إيكرمان (14 أغسطس 2013). صحيفة الغارديان. مقال: «حثّ مجتمع الاستخبارات على شرح سبب التكتّم على وثائق حسّاسة».
Guardian,
http://www.theguardian.com/world/2013/aug/14/nsa-intelligence-committeeunder-pressure-document.

81. تشارلي سافاج ولورا بواتراس (11 مارس 2013). صحيفة نيويورك تايمس. مقال: «كيف تطوّرت محكمة بسريّة، وزادت في قدرة جواسيس أميركا».
New York Times,
http://www.nytimes.com/2014/03/12/us/how-a-courts-secret-evolution-extendedspies-reach.html.

82. إميلي بيترســون (30 سبتمبر 2011). «لجنة مراسلين من أجل حريّة الصحافة». تقرير: «طي الكتمان: أسرار المحكمة العليا».
Reporters Committee for Freedom of the Press,
http://www.rcfp.org/browse-media-law-resources/news-media-law/news-media-law-summer-2011/under-seal-secrets-supreme-cour

83. كورا كورير (30 يوليو 2013). موقع «بروبابليكا». مقال: «ســجل الرئيس أوباما في قمع مسّربي وثائق الأمن القومي».
Pro Publica,
http://www.propublica.org/special/sealing-loose-lips-charting-obamas-crackdown-on-national-security-leaks

84. ليوناردو داوني جونيور وســارة رافســكي (أكتوبر 2013). «لجنة حماية الصحافيين». مقال: «التحقيقات في التسريبات والرقابة في أميركا ما بعد 11/9».
https://www.cpj.org/reports/2013/10/obama-and-the-press-us-leaks-surveillance-post-911.php.
ديفيـد بـوزن (20 ديســمبر 2013). مجلة هارفرد لو ريفيو. مقـال: «وحش ليفياثان المُسرّب: كيف تدين الحكومة وتشجّع الكشف غير المشروع عن الوثائق».
Harvard Law Review 127,
http://harvardlawreview.org/2013/12/the-leaky-leviathan-why-the-government-condemns-and-condones-unlawful-disclosures-of-information.

85. دانيـال إلســبرغ (30 مايو 2014)، صحيفة الغارديان. مقال: «ســنودن لن يحظـى بمحاكمة عادلة، وكيري على خطأ».
Guardian,
http://www.theguardian.com/commentisfree/2014/may/30/daniel-ellsberg-snowden-fair-trial-kerry-espionage-act.

86. ديفيد ديســهنو (20 يوليو 2012). وكالة أنباء «أسوشــيتد برس». مقال: «منع تشيلســاماننغ من مناقشــة أضرار «ويكيليكس»».
Associated Press,
http://seattletimes.com/html/nationworld/2018724246_apusmanningwikileaks.html

87. هناك انقسام أميركي حول تلك النقطة. سيث موتيل (15 أبريل 2014). مقال: «تغطية «وكالة الأمن القومي» تنال جائزة «بوليتزر»، لكن الأميركيّين منقسمون حول تسريبات سنودن».
Pew Research Center,
http://www.pewresearch.org/fact-tank/2014/04/15/nsa-coverage-wins-pulitzer-but-americans-remain-divided-onsnowden-Leaks

88. جوناثـان توبـاز (28 مايـو 2014). موقـع «بوليتيكـو». مقال: «جون كيري: إدوارد ســنودن هـو «جبان... وخائن»».
Politico,
http://www.politico.com/story/2014/05/edward-snowden-coward-john-kerry-msnbc-interview-nsa-107157.html

89. فوبيه غرينوود (4 يوليو 2014). صحيفة الغارديان. مقال: «وفق كلينتون، يجب أن يحظى ســنودن بالحق في الدفاع قانونياً عن نفسه في الولايات المتحدة».
Guardian,
http://www.theguardian.com/commentisfree/2014/may/30/daniel-ellsberg-snowden-fair-trial-kerry-espionageact.
Trevor Timm (23 Dec 2013), «If Snowden returned to US for trial, could court admit any NSA leak evidence?» *Boing Boing*,
http://boingboing.net/2013/12/23/snowden.html.

.90 دانيـال إلسـبرغ (30 مايو 2014)، صحيفة الغارديان. مقال: «سـنودن لن يحظـى بمحاكمة عادلة، وكيري على خطأ».

Guardian,
http://www.theguardian.com/commentisfree/2014/may/30/daniel-ellsberg-snowden-fair-trial-kerry-espionage-act.

تريفور تيم (23 ديسمبر 2013). موقع «بوينغ بوينغ». مقال: «إذا عاد سنودن إلى الولايات المتحدة للمحاكمة، هل تقبل المحكمة أي دليل بصدد تسريبات «وكالة الأمن القومي»؟

Boing Boing,
http://boingboing.net/2013/12/23/snowden.html

.91 نايت أندرسـون (13 مايو 2014)، موقع «آرس تكنيكا». مقال: «كيف أدّت رغبة عمدة في كشـف مسـتخدم بذيء لـ«تويتر»، إلى انفجار الأمر في وجهه».

Nate Anderson (13 May 2014), «How a mayor's quest to unmask a foul-mouthed Twitter user blew up in his face,» *Ars Technica,* http://arstechnica.com/tech-policy/2014/05/how-a-mayors-quest-to-unmask-a-foulmouthed-twitter-user-blew-up-in-his-face

Kim Zetter (12 Jun 2014), «ACLU sues after Illinois mayor has cops raid guy parodying him on Twitter,»
Wired, http://www.wired.com/2014/06/peoria-mayor-twitter-parody

كيـم زتـر (12 يونيو 2014)، مجلة وايرد، مقال: «دعوى قضائيّة من «الاتحاد الأميركي للحريّات المدنيّة» عن عمدة «إلينويز» لأن شرطته أغارت على منزل أحد المتفاخرين على «تويتر»».

Wired, http:// www.wired.com/2014/06/peoria-mayor-twitter-parody.

.92 جينـا بورتنوي (19 مـارس 2014). صحيفة نيويورك تايمس. مقال: «من المدّعـي العام إلى بوليس الولاية: توقف عن التقاط صور المحتجّين في قاعة بلديّة «كريس كريستي»».

New York Times,
http://www.nytimes.com/2014/08/01/world/senate-intelligence-commitee-cia-interrogation-report.html

.93 لورا بواتراس ومارسيل روزنباخ وهولغر ستارك (26 أغسطس 2013). صحيفة دير شبيغيل، مقال: «الاسم الشيفري هو «آبالاتشي»: كيف تجسّست أميركا على أوروبا والأمم المتحدة».

Der Spiegel,
http://www.spiegel.de/international/world/secret-nsa-documents-showhow-the-us-spies-on-europe-and-the-un-a-918625.html

.94 برايان روس وفيك فالتر وآنا شيشتر (9 أكتوبر 2008). شبكة «آيه بي سي نيوز». مقال: «داخل قصة التنصّت على الأميركيّين».

ABC News Nightline,
http://abcnews.go.com/Blotter/exclusive-inside-account-us-eavesdropping-americans/story?id=5987804.

.95 سـايروس فاريفـار (17 يوليو 2014). موقـع «آرس تكنيكا». مقال: «موظّفو «وكالـة الأمن القومي» تداولوا روتينيّاً صوراً عارية مأخوذة من مواد اعترضوها».

Ars Technica,
http://arstechnica.com/tech-policy/2014/07/snowden-nsa-employees-routinely-pass-around-intercepted-nude-photos.

96. سـيوبهان غورمان (23 أغسـطس 2013). صحيفة وول سـتريت جورنـال. مقال: «ضبّـاط «وكالة الأمن القومي» تجسّسوا أحياناً بدافع من الحب».
Wall Street Journal Washington Wire,
http://blogs.wsj.com/washwire/2013/08/23/nsa-officers-sometimes-spy-on-love-interests

97. وكالـة الأمـن القومي الأميركيّة (3 مايـو 2012). وثيقة: «تقرير داخلي فصلي عـن الإشراف: الفصل الأول من العام 2012».
http://www2.gwu.edu/~nsarchiv/NSAEBB/NSAEBB436/docs/EBB-044.pdf.

98. تتعمّد «وكالة الأمن القومي» عدم أتمتة نظام التدقيق الداخلي، ما يعني أنها تستطيع أن تكتشف من التجاوزات بقدر عدد الأشـخاص التي تـوكل إليهم تلك المهمّة. مارسي ويلر (20 أغسـطس 2013). مقـال: «إذا ارتكبت «وكالة الأمن القومي» اعتداءات فاضحة على قاعدة بياناتها، ثم لم يكتشف أحد الأمر، أيكون قد حدث فعليّاً؟».
Empty Wheel,
http://www.emptywheel.net/2013/08/20/if-nsa-commits-database-query-violations-but-nobodyaudits-them-do-they-really-happen.

99. شوان آشر (5 يناير 2012). موقع «ليتر أوف نوتس». رسالة: «وككل الفاسدين، إنّ نهايتك تقترب».
Letters of Note,
http://www.lettersofnote.com/2012/01/king-like-all-fraudsyour-end-is.html

100. مجلس الشـيوخ الأميركي (26 أبريل 1976). وثيقة حكوميّة: «التقرير النهائي للجنة المنتدبة لدراسة عمليات الحكومة المتّصلة بنشاطات الاستخبارات. الكتاب الثاني: **نشاطات الاستخبارات وحقوق الأميركيّين**».
https://archive.org/details/finalreportofsel02unit

ميتشيل101. شميدت وكولن مويبيهان (24 ديسمبر 2012). صحيفة نيويورك تايمس. مقال: «وثائق تظهر أن عملاء الـ«إف بي آي» لمكافحة الإرهاب، ترصّدوا 'حركة احتلوا وول ستريت'».
New York Times,
http://www.nytimes.com/2012/12/25/nyregion/occupy-movement-was-investigated-by-fbi-counterterrorism-agents-records-show.html

بو هوداي (9 يونيو 2013)، موقع «سورس ووتش». مقال: «رقابة الحكومة لـ'حركة احتلوا وول ستريت'».
Sourcewatch,
http://www.sourcewatch.org/index.php/Government_Surveillance_of_Occupy_Movement.

102. شـارلي سافاج وسكوت شـاين (16 ديسـمبر 2009). صحيفة نيويورك تايمس. مقال: «التجسّس بطريقة مهينة على الأميركيّين».
New York Times,
http://www.nytimes.com/2009/12/17/us/17disclose.html.

103. «الاتحـاد الأميركـي للحريّات المدنيّة» (25 أكتوبر 2006). وثيقة: ««الاتحـاد الأميركي للحريّات المدنيّة» يعرّي رقابة الـ«إف بي آي» لنشطاء السلام في ولاية «ماين»».
https://www.aclu.org/national-security/aclu-uncovers-fbi-surveillance-maine-peace-activists

104. «الاتحاد الأميركي للحريّات المدنيّة» (29 يونيو 2010). وثيقة: «الرصد البوليسي لحرية التعبير: رقابة الشرطة وتدخّله في نشاط يحميه التعديل الأول في الدستور».
https://www.aclu.org/files/assets/Spyfiles_2_0.pdf.

لينـدا ي. فيـشر (2004). مجلـة آريزونا لو ريفيو. مقـال: «الإدانة بالترابط التعبيري: التصنيف السـياسي، الرقابة وخصوصيّة المجموعات».
Arizona Law Review 46,
http://www.arizonalawreview.org/pdf/46-4/46arizlrev621.pdf.
US Department of Justice (Sep 2010), «A review of the FBI's investigations of certain domestic advocacy groups,»

http://www.justice.gov/oig/special/s1009r.pdf.

105. غلـين غرينوالد ومرتضى حسـين (9 يوليو 2014). موقع «إنترسـبت». مقال: «تحـت الرقابة: لقاءات مع قادة أميركيّين- مسلمين تراقبهم الـ«إف بي آي» و«وكالة الأمن القومي»».

Intercept,
https://firstlook.org/theintercept/article/2014/07/09/under-surveillance

106. «وكالـة أسوشـيتد برس» (2012). مقال: «إضاءات من أداة للتحقيق الاسـتقصائي فائـزة بجائزة «بوليتزر» للصحافة، على عمليات الرقابة التي يجريها بوليس نيويورك».

http://www.ap.org/media-center/nypd/investigation
, and http://www.ap.org/Index/AP-In-The-News/NYPD

107. كاييد كروكفورد (25 مايو 2014). موقع «برايفسي إس أو إس». مقال: «وثائق تثبت أنّ «مركز الانصهار» في بوسطن «لمكافحة الإرهاب»، وثّق «حركة احتلوا...» في بوسطن، بشكل وسواسي».

Privacy SOS,
http://privacysos.org/node/1417

كارول روز وكاييـد كروكفـورد (30 مايو 2014)، مقال: «عندما تتجسّـس الشرطة على حريّة التعبير، تعاني الديمقراطيّة».

http://cognoscenti.wbur.org/2014/05/30/boston-regional-intelligence-center-carol-rosekade-crockford.

108. لوك أونيل (13 أغسـطس 2014). شبكة «آن بي سي نيوز». مقال: «»الأخ الكبير» لـ«بينتاون»: كيف استخدم بوليس مدينة بوسطن تقنيّة التعرّف إلى الوجوه للتجسّس على آلاف المشاركين في مهرجان موسيقي».

Noisey,
http://noisey.vice.com/blog/beantowns-big-brother

109. ليزا مايرز ودوغلاس باسـترناك وريتش غارديلا (14 ديسـمبر 2015). شـبكة «آن بي سي نيوز». مقال: «هل يتجسّس البنتاغون على أميركا»؟

Lisa Myers, Douglas Pasternak,
and Rich Gardella (14 Dec 2005), «Is the Pentagon spying on Americans?» *NBC News,*
http://www.nbcnews.com/id/10454316/ns/nbc_nightly_news_with_brian_williamsnbc_news_investigates/t/pentagon-spying-americans.

110. غلـين غرينوالد ورايـن غريم وراين غالاهار (26 نوفمبر 2013). صحيفة **هافنغتون بوسـت**. مقال: «وثائق سريّة جداً تظهر تجسّـس «وكالة الأمن القومي» على عادات مشـاهدة أشرطة الجنس الإباحي، كجزء من خطة لإفقاد «المُجذّرين» مصداقيّتهم».

Huffington Post,
http://www.huffingtonpost.com/2013/11/26/nsa-porn-muslims_n_4346128.html

111. كريس هامبي (6 أكتوبر 2014). مقال: «الحكومة تستخدم اسم امرأة في صنع صفحة مزيفة على «فيسبوك»».
http://www.buzzfeed.com/chrishamby/government-says-federal-agents-can-impersonate-woman-online

112. ويليـام بندر (23 فبراير 2010). صحيفة **فيلادلفيا إنكوايرر**. مقـال: «نقلاً عن محامي: ل. ماريون صامت بصدد عدد من الصور الملتقطة بكاميرا الـ«ويب»».

Philadelphia Inquirer,
http://articles.philly.com/2010-02-23/news/24957453_1_webcam-laptops-students

113. إريك ليشتبلاو وجيمس ريزن (23 يونيو 2006). صحيفة **نيويورك تايمس**. مقال: «تلاعبت الولايات المتحدة سراً ببيانات البنوك بذريعة محاربة الإرهاب».

New York Times,
http://www.nytimes.com/2006/06/23/washington/23intel.html.

لويـك إيسر (3 يوليـو 2014). مجلة **عالم الكومبيوتر**. مقال: «محكمة «الاتحاد الأوروبي» تطالب بشـفافية أكبر في البرنامج الأميركي- الأوروبي لتتبع أموال الإرهاب».

PC World,
http://www.pcworld.com/article/2450760/eu-court-orders-more-transparency-over-useu-terrorist-finance-tracking-program.html

مونيكا إرميت (23 أكتوبر 2013). مقال: «البرلمان الأوروبي: لا استمرار في نقل بيانات البنوك إلى التحقيقات الأميركيّة عن الإرهاب».
Intellectual Property Watch,
http://www.ip-watch.org/2013/10/23/european-parliament-no-more-bank-data-transfers-to-us-for-anti-terror-investigations

114. «الاتحاد الأميركي للحريّات المدنيّة». (7 مارس 2002). تقرير: «كيف يعزّز «قانون باتريوت» تفويضات «تسلّل وتلصص» المعطاة إلى قوى إنفاذ القانون».
https://www.aclu.org/technologyand-liberty/how-usa-patriot-act-expands-law-enforcement-sneak-and-peek-warrants.

تيم تريفور (26 أكتوبر 2011). «مؤسّسة الحدود الإلكترونيّة». مقال: «بعد عشر سنوات على «قانون باتريوت»، عرض للتشريعات الثلاثة الأكثر مساساً بحياة المواطنين الأميركيّين العاديّين».
Electronic Frontier Foundation,
https://www.eff.org/deeplinks/2011/10/ten-years-later-look-three-scariestprovisions-usa-patriot-act.

115. تتشارك «وكالة الأمن القومي» المعلومات مع «وكالة مكافحة المخدّرات» منذ سبعينيات القرن العشرين. جيمس بامفورد (2008)، كتاب: **المصنع الخفي: وكالة الأمن القومي الفائقة الخفاء من 9/11 إلى التنصّت على أميركا**. دار «دوبلداي» للنشر.
The Shadow Factory: The
Ultra-Secret NSA from 9/11 to Eavesdropping on America, Doubleday,
http://books.google.com/books?id=8zJmxWNTxrwC

116. جون شيفمان وكريستينا كوك (5 أغسطس 2013). وكالة «رويترز» للأنباء. مقال: «الحكومة توجّه عملاء بإخفاء برنامج استُخدِم في التحقيق مع أميركيّين».
Reuters,
http://www.reuters.com/article/2013/08/05/us-dea-sod-idUSBRE97409R20130805

هاني فاخوري (6 أغسطس 2013). «مؤسّسة الحدود الإلكترونيّة». تقرير: «تشارك في البيانات بين «وكالة الأمن القومي» و«وكالة مكافحة المخدّرات»، يؤدي إلى استعمال معلومات الرقابة في التحقيقات العاديّة».
Electronic Frontier Foundation,
https://www.eff.org/deeplinks/2013/08/dea-and-nsa-team-intelligence-laundering.
John Shiffman and David Ingram (7 Aug 2013), «IRS manual detailed DEA's use of hidden intel evidence,» Reuters,
http://www.reuters.com/article/2013/08/07/us-deairs-idUSBRE9761AZ20130807.

117. قدّم مُطلِق صافرة الإنذار بيل بيني الوصف التالي: «... عندما لا تتمكن من استعمال البيانات، يجب عليك صنع بنية موازية [ما يعني] أنك تستعمل ما تعدّه وسائل تحقيق عاديّة، [ثم] تعثر على البيانات. لكنك تملك تلميحاً معيّناً. إذ أخبرتك «وكالة الأمن القومي» أين توجد تلك البيانات...». آليكس أوبراين (30 سبتمبر 2014). تقرير: «مدير متقاعد للتكنولوجيا في «وكالة الأمن القومي» يشرح وثائق سنودن».
http://www.alexaobrien.com/secondsight/wb/binney.html

118. برايان كريبس (14 أكتوبر 2014). موقع «كريبس أو سكيوريتي». مقال: «محامو «درب الحرير» يجدون ثغرات في رواية الـ«إف بي آي»».
Krebs on Security,
http://krebsonsecurity.com/2014/10/silk-road-lawyers-poke-holes-in-fbis-story

119. روب إيفانــز وبول لويس (26 أكتوبر 2009). صحيفة الغارديان. مقال: «تحدي قوات الشرطة بشــأن صنع ملفات عن محتجّين ملتزمين بالقوانين».

Guardian,
http://www.theguardian.com/uk/2009/oct/26/police-challenged-protest-files

120. غـوردون راينر وريتشــارد آلليياني (12 أبريـل 2008). صحيفة التلغراف. مقال: «حالات تجسّــس المجلس تلامس الألف شهريّاً».

Telegraph,
http://www.telegraph.co.uk/news/uknews/1584808/Council-spy-cases-hit-1000-a-month.html

ســارة ليـول (24 أكتوبر 2009). صحيفــة نيويورك تايمس. مقــال: «ارتياب البريطانيّين مـن الرقابة على القضايا الصغيرة».

New York Times,
http://www.nytimes.com/2009/10/25/world/europe/25surveillance.html

121. جيمــس بامفورد (16 ســبتمبر 2014). صحيفة نيويورك تايمس. مقال: «فضيحــة إسرائيل و«وكالة الأمن القومي»».

New York Times,
http://www.nytimes.com/2014/09/17/opinion/israels-nsa-scandal.html

122. هنــاك مقــال يثير تلك النقطــة تحديداً. دانيــال دايفيس (23 ســبتمبر 2014). مقال: «كل شــخص يعمل في المعلوماتيّة، وكل مدير...».
http://crookedtimber.org/2014/09/23/every-single-it-guy-every-single-manager

123. هيلاري رودهام كلينتون (21 يناير 2010)، خطاب «حريّة الإنترنت». مجلة فورين بوليسي.
Foreign Policy,
http://www.foreignpolicy.com/articles/2010/01/21/internet_freedom

124. وزارة الخارجية الأميركية (2014). تقرير: «حريّة الإنترنت».
http://www.state.gov/e/eb/cip/netfreedom/index.htm

125. هيئة الإذاعة البريطانيّة (2 يونيو 2014). مقال: ««نحن مراقبون»، يقول المصريون على الــسوشال ميديا»».
BBC News,
http://www.bbc.com/news/blogs-trending-27665568.

126. جايشري باجورا (5 يونيو 2014). صحيفة إنديا رييل تايم. مقال: «سنودن وتلصص الهند».
India Real Time,
http://blogs.wsj.com/indiarealtime/2014/06/05/indias-snoopingand-snowden.

127. شــانون تييزي (28 مــارس 2014). موقع «ديبلومات». مقــال: «الصين تندّد بالنفاق الأميركي في التجسّــس السبراني».
http://thediplomat.com/2014/03/china-decriesus-hypocrisy-on-cyber-espionage

وكالة «شــينخوا» للأنباء (11 يوليو 2014). صحيفة تشــاينا دايلي. مقال: «بوتين يصف ممارســات الرقابة الأميركيّة بأنّها «نفاق كامل»».

China Daily,
http://www.chinadaily.com.cn/world/2014-07/11/content_17735783.htm

128. مارك زوكربرغ (13 مارس 2014)، تدوين إلكتروني على «فيسبوك»: «العالم يغدو أكثر تعقيداً...».
Facebook,
https://www.facebook.com/zuck/posts/10101301165605491.

الفصل 8: العدالة التجاريّة والمساواة

1. «مكتب المدّعي العام في «مينسوتا» (19 يناير 2012). قضيّة: «المدّعي العام سوانسون يقاضي «آكريتف هيلث» لانتهاكها خصوصيّة المرضى».
http://www.ag.state.mn.us/Consumer/PressRelease/120119AccretiveHealth.asp

2. توني كينيدي وموراليرنر (31 يوليو 2012). صحيفة **ستار تريبيون**. مقال: «حظر «آكريتف» في «مينسوتا»».
Star-Tribune,
http://www.startribune.com/lifestyle/health/164313776.html.

3. كايت كراوفورد وجايسون شولتز (2014). مجلة **بوسطن كوليدج لو ريفيو**. ورقة: «بيانات ضخمة وعملية متلائمة معها: نحو إطار لتصحيح مخاطر الخصوصيّة التوقعيّة».
http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2325784.

4. مارك هوكشتاين (26 يونيو 2000). موقع «أميركان بانكر». مقال: «بنك «ويلز فارغو» يمحو وصلة إلكترونيّة بعد مقاضاته من «آكرون»».
American Banker,
http://www.americanbanker.com/issues/165_119/-128168-1.html
غاري هيرنانديز وكاثرين إيدي وجويل ماتشمور (خريف 2001). مجلة **ساوثرن ميثوديست يونيفرستي لو ريفيو**. ورقة: «ممارسة «عبر خطوط الويب» هي تمييز غير عادل في الفضاء السبراني».
http://heinonline.org/HOL/LandingPage?collection=journals&handle=hein.journals/smulr54&div=91.

5. بيل دافيدو (5 مارس 2014). مجلة آتلانتيك. مقال: «ممارسة «عبر الخطوط الحمر» في القرن 21».
Atlantic,
http://www.theatlantic.com/business/archive/2014/03/redlining-for-the-21st-century/284235.

6. مايكل ليدتكه (22 يونيو 2000). صحيفة **لوس أنجلوس تايمس**. مقال: «دعوى قضائيّة بشأن استخدام «ويلز فارغو» الإنترنت لترويج التمييز».
Los Angeles Times,
http://articles.latimes.com/2000/jun/22/business/fi-43532.
رونا أبرامسون (23 يونيو 2000). مجلة **عالم الكومبيوتر**. مقال: «إدانة «ويلز فارغو» بممارسة سياسة «عبر الخطوط الحمر» على الإنترنت».
Computer World,
http://www.computerworld.com/article/2596352/financial-it/wells-fargo-accused-of--redlining--on-the-net.html

7. مارسيا ستيبانك (3 أبريل 2000). مجلة **بلومبرغ ويك**. مقال: «عبر خطوط الويب».
كايسي جونستون (10 أكتوبر 2013). موقع «آرس تكنيكا». مقال: «هل رُفض طلبك ذلك القرض؟ عليك أن تشكر جمع المعلومات على الـ«ويب»».
Ars Technica,
http://arstechnica.com/business/2013/10/denied-for-that-loan-soon-you-may-thank-online-data-collection.

8. «المكتب التنفيذي للرئاسة» (1 مايو 2014). تقرير: «البيانات الضخمة: التقاط الفرصة والحفاظ على القيم».
http://www.whitehouse.gov/sites/default/files/docs/big_data_privacy_report_may_1_2014.pdf.

9. يجب على «أوبر» تعديل أسعارها كي لا تتصادم مع قيود ولاية «نيويورك» التي تحظر رفع الأسعار أثناء حالات الطوارئ. مايك آيزاك (8 يوليو 2014). صحيفة **نيويورك تايمس**. مقال: «التوصّل إلى اتفاقيّة بين شركة «أوبر» وولاية نيويورك بشأن رفع الأسعار في أحوال الطوارئ».
New York Times,

http://bits.blogs.nytimes.com/2014/07/08/uber-reaches-agreement-with-n-yon-surge-pricing-during-emergencies.

بيتر هيلمر (12 أغسطس 2014). مجلة فوربس. مقال: «شركة «أوبر»: جيّدة تماماً، ولكن ليس كفاية».

Forbes,

http://www.forbes.com/sites/peterhimler/2014/08/12/uber-socool-but-so-uncool

10. جنيفر فالنتينو- دوفريز وجيرمي سنغير- فاين وآشكان سلطاني، وول ستريت جورنال. مقال: «مواقع شبكيّة تقدّم أسعاراً مختلفة في صفقات تعتمد على المعلومات عن المستخدم».

Wall Street Journal,

http://online.wsj.com/news/articles/SB100014241278873237772045781893918 13881534.

Michael Schrage (29 Jan 2014), «Big data's dangerous new era of discrimination,»

Harvard Business Review,

http://blogs.hbr.org/2014/01/big-datas-dangerous-new-era-of-discrimination

11. إميلي ستيل وجوليا أنغوين (4 أغسطس 2010). صحيفة وول ستريت جورنال. مقال: «في الحدود القصوى لتقنيات الـ«ويب»، ليس إغفال الهوية سوى اسم».

Wall Street Journal,

http://online.wsj.com/news/articles/SB10001424052748703294904575385532109190198

12. جنيفر فالنتينو- دوفريز وجيرمي سنغير- فاين وآشكان سلطاني، وول ستريت جورنال. مقال: «مواقع شبكيّة تقدّم أسعاراً مختلفة في صفقات تعتمد على المعلومات عن المستخدم».

Wall Street Journal,

http://online.wsj.com/news/articles/SB10001424127887323777204578189391813881534

13. بام ديكسون وروبرت غيلمان (2 أبريل 2014). «منتدى الخصوصيّة العالمي». مقال: «سجل لأميركا كزبون: كيف تهدّد السجلات السريّة للمستهلك خصوصيّتك ومستقبلك».

World Privacy Forum,

http://www.worldprivacyforum.org/wp-content/uploads/2014/04/WPF_Scoring_of_America_April2014_fs.pdf

14. جيسيكا فاسيلارو (7 مارس 2011). صحيفة وول ستريت جورنال. مقال: «الموجة المقبلة في التلفزة: ضبط الإرسال ليكون أنت».

Wall Street Journal,

http://online.wsj.com/articles/SB1000142405274870428830457617125168994435 0

15. دانا ماتيولي (23 أغسطس 2012). صحيفة وول ستريت جورنال. مقال: «في «أوربتز»، مستخدمو الـ«ماك» يواجهون استضافة أعلى سعراً».

Wall Street Journal,

http://online.wsj.com/news/articles/SB100014240527023044586045774888226 67325882

16. بيل ماكغي (3 أبريل 2013). صحيفة يو إس إيه توداي. مقال: «هل عروض السفر تتغيّر وفق تاريخ تصفّحك للإنترنت»؟

USA Today,

http://www.usatoday.com/story/travel/columnist/mcgee/2013/04/03/do-travel-deals-change-based-on-your-browsing-history/2021993.

17. لوشيا موسيس (2 أكتوبر 2013). مجلة آد ويك. مقال: «يحرص المسوّقون على معرفة متى تشعر المرأة بأن جاذبيتها أقل: ما هي الرسائل التي يجب نقلها، ومتى يجب إرسالها».

Adweek,

http://www.adweek.com/news/advertising-branding/marketers-should-take-note-when-women-feel-least-attractive-152753.
Kim Bates (4 Oct 2013), «Beauty vulnerability: What got lost in translation,» *Adweek*, http://www.adweek.com/news/advertising-branding/beauty-vulnerabilitywhat-got-lost-translation-152909

18. «فرانك ن. مجيد أسوسيتس» (2011). «رابطة صحف أميركا». مقال: «كيف تتسوّق أميركا وتنفق في 2011».
http://www.naa.org/docs/newspapermedia/data/howamericashopsandspends_2011.pdf

19. كاتي لوبوسكو (27 أغسطس 2013). شبكة «سي آن آن». مقال: «قائمة أصدقائك على «فيسبوك»، تغيّر حسابك في بطاقة الائتمان».
CNN,
http://money.cnn.com/2013/08/26/technology/social/facebook-credit-score.

20. كاري تغردين (21 ديسمبر 2008). صحيفة آتلانتا جورنال- كونستيتيوشن. مقال: «شركات بطاقات الائتمان تغيّر سقوف بطاقاتها: تكون أقل للبعض وفقاً لأمكنة مشترياتهم».
Atlanta Journal-Constitution,
https://web.archive.org/web/20110728060844/http://www.ajc.com/news/content/business/stories/2008/12/21/creditcards_1221.html

21. أوسكار غندي جونيور (1993). كتاب: **الفرز بواسطة الرؤية الشاملة: الاقتصاد السياسي للمعلومات الشخصيّة**. دار «ويست فيو برس».
The Panoptic Sort: A Political Economyof Personal Information, Westview Press,
http://books.google.com/books?id=wreFAAAAMAAJ.

22. ورقة البحث التالية تسرد الطرق المتنوّعة التي تتبعها الشركات في التمييز استناداً إلى «البيانات الضخمة». سولون بروكاس وآندرو سلبست (14 سبتمبر 2014). «سوشال ساينس ريسرش نتورك». ورقة بحث: «التفاوت في تأثير «البيانات الضخمة»».
Social Science Research Network,
http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2477899

23. كايسي جونستون (13 أغسطس 2014). موقع «آرس تكنيكا». مقال: «المطعم الذي فتشت عليه في «غوغل» يستخدمه أيضاً في استخراج معلومات عنك».
Ars Technica,
http://arstechnica.com/staff/2014/04/when-the-restaurant-you-googled-googles-you-back

24. هيلاري أوزبورن (13 أغسطس 2012). صحيفة **الغارديان**. مقال: «شركة «أفيفا» للسيارات تجرّب تقنيّة للتأمين بالهاتف الذكي».
Guardian,
http://www.theguardian.com/money/2012/aug/13/aviva-trial-smartphone-car-insurance-technology
راندال ستروس (25 نوفمبر 2012)، صحيفة **نيويورك تايمس**. مقال: «إذا كنت سائقاً ماهراً، دعنا نقيّم ذلك».
New York Times,
http://www.nytimes.com/2012/11/25/business/seeking-cheaper-insurance-driversaccept-monitoring-devices.html.
براد توتيل (6 أغسطس 2013). مجلة تايم. «السائق المساعد هو «البيانات الضخمة»: شركات ضمان السيّارات تروّج أدوات ترصد عادات القيادة».
Time,
http://business.time.com/2013/08/06/big-data-is-my-copilot-auto-insurers-push-devices-that-track-driving-habits.

25. نانسي غورينغ (7 يوليو 2017). موقع «ساست ورلد». مقال: «هذه الشركة وفّرت ثلاثمائة ألف دولار من أموال الضمان الصحي، بإعطاء موظّفيها سوارات «فِت بت»».

CiteWorld,
http://www.citeworld.com/article/2450823/internet-of-things/appirio-fitbit-experiment.html

26. لي كراين (5 سبتمبر 2013). مجلة ديجيتال تريند. مقال: «درس الرياضة سيصبح أسوأ لغير محبي الرياضة».

Digital Trends,
http://www.digitaltrends.com/sports/gym-class-is-about-to-get-even-worse-for-the-athletically-dis-inclined

إميلي ميلز (28 مايو 2014). موقع «ليدر- تليغرام». مقال: «طلاب ثانويّة «ميموريال» بلغوا ذروة لياقتهم بفضل مجسّات لنبضات القلب».

Leader-Telegram,
http://www.leadertelegram.com/news/front_page/article_ec2f0b72-e627-11e3-ac95-0019bb2963f4.html

Katie Wiedemann (14 Aug 2014), «Heart rate monitors now required in Dubuque P.E. classes,» KCRG,
http://www.kcrg.com/subject/news/heart-rate-monitors-nowrequired-in-dubuque-physical-education-classes-20140814

27. جويل شيشتمان (14 مارس 2012). صحيفة وول ستريت جورنال. مقال: «سجل: برنامج من شركة «آتش بي» استطاع التنبّؤ بالموظفين الموشكين على ترك الشركة».

Wall Street Journal,
http://blogs.wsj.com/cio/2013/03/14/book-hp-piloted-program-to-predict-which-workers-would-quit

28. تعطي الورقة التالية تحليلًا ممتازاً للرقابة في مواقع العمل. آليكس روكسنبلات وتامارا كنزي ودانا بويد (8 أكتوبر 2014). موقع «داتا أند سوسيتي ريسرتش إنستيتيوت».

Data and Society Research Institute,
http://www.datasociety.net/pubs/fow/WorkplaceSurveillance.pdf

29. إلين مسمير (31 مارس 2010). موقع «نتورك ورلد». مقال: «هل تحس أنك مراقب في العمل؟ الأرجح أنّك محق».

Network World,
http://www.networkworld.com/article/2205938/data-center/feel-like-you-re-being-watched-at-work--youmay-be-right.html.

جوش بيرسن (25 يونيو 2014). مجلة فوربس. مقال: «الذات المقوّمة كميّاً: لنتحدث عن الموظّف المقوّم كميّاً».

Forbes,
http://www.forbes.com/sites/joshbersin/2014/06/25/quantified-self-meet-the-quantified-employee.

30. دون بيك (20 نوفمبر 2013). مجلة آتلانتيك. مقال: «إنّهم يراقبونك في العمل».

Atlantic,
http://www.theatlantic.com/magazine/archive/2013/12/theyre-watching-you-at-work/354681

هانا كوشلر (17 فبراير 2014). صحيفة فاينَنشال تايمس. مقال: «روّاد التقنية يراقبوننا في العمل».

Financial Times,
http://www.ft.com/intl/cms/s/2/d56004b0-9581-11e3-9fd6-00144feab7de.html

31. يعتبر المقال التالي مراجعة ممتازة عن تقنيات الرقابة في أمكنة العمل وتأثيراتها في الخصوصيّة. كوري أ. سيوشيتي (2010). جامعة دنفر. بحث: «رب العمل المتنصّت: إطار للقرن 21 عن ترصّد الموظّف».

University of Denver,
http://www.futureofprivacy.org/wp-content/uploads/2010/07/The_Eavesdropping_Employer_%20A_Twenty-First_Century_Framework.pdf

32. حدثتني إحدى الصديقات عن مشـاعرها حيال الإعلان المُشَـخْصَن. قالت إنّها امرأة متقدّمة في السـن، وتتلقى باستمرار إعلانات عن عمليات تجميل، أدوية لعلاج أمراض «الكبار» وأشياء أخرى تذكّرها دوماً بعمرها. وتجد ذلك غير مريح. لين سـودبري وبيتر سـيمكوك (2008). مقال: «تابو كبار السـن؟ إعلانات مستندة إلى العمر، النظرة الذاتيّة إلى العمر والمستهلك الكبير السنّ».
European Advances in Consumer Research 8,
http://www.acrwebsite.org/volumes/eacr/vol8/eacr_vol8_28.pdf.

33. ديبوراه س. بيل (7 فبراير 2014). «إعلان د. ديبوراه س. بيل «مؤسّسـة حقوق الخصوصيّة للمرضى» بدعم من اسـتجواب المدّعين للحصول على ملخّص جزئي للحكم». في «قضية الكنيسـة التوحيديّة الأولى وفريقها ضد «وكالة الأمن القومي» وفريقها»، في محكمة المقاطعة الشمالية في كاليفورنيا.
https://www.eff.org/files/2013/11/06/allplaintiffsdeclarations.pdf.

34. آنـدرو أودليزكـو (5-6 يونيـو 2014). «مؤتمـر بحّاثـة قوانـين الخصوصيّة» في واشـنطن. بحـث: «نهاية الخصوصيّة وبذور دمار الرأسماليّة».
http://www.law.berkeley.edu/plsc.htm

35. 713 بادي كامن (5 يوليو 2001). صحيفة تورنتو سـتار. مقال: «هل اعتقدت بأنّ محرّكات البحث تقدّم نتائج محايدة؟ فكّر ثانية».
http://www.commercialalert.org/issues/culture/search-engines/so-you-thought-search-engines-offer-up-neutralresults-think-again

36. غاري روسكين (16 يوليو 2001). رسالة إلى دونالد كلارك، «اللجنة الفيدراليّة للتجارة» عن: شكوى بالتلاعب الإعلانـي ضـد شركات «ألتافيسـتا»، «إيـه أو آل تايم ورنـر»، «دايركت هـت تكنولوجيـز»، «آي وون»، «لوك سمارت»، «مايكروسوفت» و«تيرا لايكوس».
http:// www.commercialalert.org/PDFs/SearchEngines.pdf
هيثر هيبسـلي (27 يونيو 2002). رسـالة إلى غاري روسكين، عن: شكوى تطلب التحقيق مع شركات محرّكات البحث على الإنترنت بشأن الموضعة المدفوعة وبرامج الاشتمال المدفوعة. «اللجنة الفيدرالية للتجارة».
Commission,
http://www.ftc.gov/sites/default/files/documents/closing_letters/commercial-alert-response-letter/commercialalertletter.pdf

37. داني سـوليفان (30 مايو 2012). موقع «ماركيتنغ لاند». مقال: «بعد أن عدّها شـيطاناً، بات «غوغل» يتبنى «الاشتمال المدفوع»».
Marketing Land,
http://marketingland.com/once-deemed-evil-google-now-embraces-paid-inclusion-13138

38. مايكل كوني (25 يونيو 2013). موقع «نتورك ورلد». مقال: «طلبت «اللجنة الفيدراليّة للتجارة» من «غوغل» و«ياهوو» و«بينغ» وغيرهم، تحسين طريقة تمييز الإعلانات في نتائج تفتيش المحتوى على الإنترنت».
Network World,
http://www.networkworld.com/community/blog/ftc-tells-google-yahoo-bingothers-better-differentiate-ads-web-content-searches
ماري ي. أنغل (24 يونيو 2013). «اللجنة الفيدراليّة للتجارة». «رسـالة قضائيّة عن: ممارسـات الإعلان على محرّكات البحث».
http://www.ftc.gov/sites/default/files/attachments/press-releases/ftc-consumerprotection-staff-updates-agencys-guidance-search-engine-industryon-need distinguish/130625searchenginegeneralletter.pdf

39. جوش كونسـتين (3 أكتوبر 2012). موقع «تيك كرانش». مقال: «راهناً، صار «فيسـبوك» يتيح للمستخدمين الأميركيّين دفع 7 دولارات مقابل إيصال تدويناتهم إلى عدد أكبر من الأصدقاء».

Tech Crunch,
http://techcrunch.com/2012/10/03/us-promoted-posts

40. روبرت بوند وآخرون (13 سبتمبر 2012). مجلة نايتشر العلميّة. بحث: «وضع 61 مليون شخص قيد تجربة في التأثير الاجتماعي والتحشيد السياسي».

Nature 489,
http://www.nature.com/nature/journal/v489/n7415/full/nature11421.html

41. استقصى جوناثان زيترين ذلك الاحتمال. جوناثان زيترين (1 يونيو 2014). موقع «نيو ريبابليك». مقال: «يستطيع «فيسبوك» أن يحسم الانتخابات من دون أن يلاحظه أحد».

New Republic,
http://www.newrepublic.com/article/117878/information-fiduciary-solution-facebook-digital-gerrymandering

42. كانت مجموعة من الانتخابات الأميركيّة متقاربة. وبفارق 0.01 % من الأصوات، كان آل غور ليفوز على جورج بوش في 2000. وفي 2008، كان آل فرانكلين ليهزم نورمان كولمان في انتخابات مقعد مجلس الشيوخ عن ولاية «مينسوتا»، لو تغيّر اتجاه 312 صوتاً.

43. 721 روبرت إيبشتاين (مايو 2013). مقال: «ديموقراطيّة في خطر: التلاعب بنتائج البحث على الإنترنت، بإمكانه تغيير تفضيلات المصوّتين دون أن يدروا».

25th Annual Meeting of the Association for Psychological Science, Washington, D.C.,
http://aibrt.org/downloads/EPSTEIN_and_Robertson_2013-Democracy_at_Risk-APS-summary-5-13.pdf

44. «عندما تكون كمية المعلومات فائقة الضخامة والشفافيّة والاختراق؛ لا يلزمك إطلاقاً سوى استعمال الحقائق المثبتة لانخراط في بروباغندا مطلقة وتحويل الناس إلى قطعان كلياً». اقتباس من دان غيير نقله جوناثان زيترين (20 يونيو 2014)، مجلة منتدى هارفرد للقانون، بحث: «انتخابات مخطّطة».

Harvard Law Review Forum 127,
http://harvardlawreview.org/2014/06/engineering-an-election

45. آي ويي ويي (17 أكتوبر 2012). موقع «نيوستاتس مان». مقال: «مجاميع الصين المدفوعة الأجر: حزب الخمسين سنتاً».

New Statesman,
http://www.newstatesman.com/politics/politics/2012/10/china%E2%80%99s-paid-trolls-meet-50-cent-party

غاري كينغ وجنيفر بان ومارغريت ي. روبرتس (22 أغسطس 2014). مجلة ساينس العلميّة. بحث: «الحجب بواسطة التخطيط المعكوس: اختبار عشوائي وملاحظة المشارك».

Science 345,
http://www.sciencemag.org/content/345/6199/1251722.

46. فيليب إلمر- ديويت (16 إبريل 2013). مجلة فورتشن. مقال: «تدّعي «سامسونغ» أنّها ليست كذلك».

Fortune,
http://fortune.com/2013/04/16/say-it-aint-so-samsung

47. برايان هورلينغ وماثيو كوليك (4 ديسمبر 2009)، «المدوّنة الإلكترونيّة الرسميّة لـ«غوغل»، مقال: «بحث مُشَخصَن للجميع».

Google Official Blog,
http://googleblog.blogspot.com/2009/12/personalized-search-for-everyone.html

تيــم آدامــز (19 يناير 2013)، صحيفة الغارديان، مقال: «محرّك «غوغل» ومســتقبل البحث: آميت ســنغال والرسم البياني للمعرفة».
Guardian,
http://www.theguardian.com/technology/2013/jan/19/google-search-knowledge-graph-singhal-interview

48. «شبكة شيكيتا الإلكترونيّة للإعلان» (7 يناير 2013). مقال: «قيمة الموضعة في نتائج «غوغل»».
https://cdn2.hubspot.net/hub/239330/file-61331237-pdf/ChitikaInsights-ValueofGoogleResultsPositioning.pdf

49. جوزيــف تورو (2013). كتاب: **أنت اليومي: الصناعة الجديدة للإعلانات تحدّد هويّتك وقيمتك**. «مطبعة جامعة يال».
http://yalepress.yale.edu/yupbooks/book.asp?isbn=9780300165012

50. إيلي باريزر (2011)، كتاب: **فقاعة الفلتر: ما الذي تخفيه الإنترنت عنك؟**. كتب «بنغوين».
http://www.thefilterbubble.com.

51. كاس زونشتاين (2009). كتاب: **الجمهورية. كوم، 2.0**. مطبعة جامعة برنستون.
http://press.princeton.edu/titles/8468.html

52. للإنصاف، ذلك الميل أكثر قدماً وعموميّة من الإنترنت. روبرت د. بوتمان (200)، كتاب: **لعب البولينغ وحيداً: انهيار المجتمع الأميركي وتجدّده**. «دار سايمون وشوستر».
http://bowlingalone.com

53. آدم د. أي. كرامــر وجايمــي ي. غولوري وجيفري ت. هانكــوك (17 يونيو 2014). بحث: «دلائل تجريبيّة عن حدوث عداوات عاطفيّة ضخمة بواسطة شبكات التواصل الاجتماعي».
Proceedings of the National Academy of Sciences of the United States of America 111,
http://www.pnas.org/content/111/24/8788.full

54. لوشــيا موســيس (2 أكتوبر 2013). مجلة آد ويك. مقال: «يحرص المسوّقون على معرفة متى تشعر المرأة بأن جاذبيتها أقل: ما هي الرسائل التي يجب نقلها، ومتى يجب إرسالها».
Adweek,
http://www.adweek.com/news/advertising-branding/marketers-should-take-note-when-women-feel-least-attractive-152753.

55. مارك بوكانان (17 أغسطس 2007). مجلة ستراتيجي+ بيزنس. مقال: «علم الإشارات المرهفة».
strategy+business magazine,
http://web.media.mit.edu/~sandy/Honest-Signals-sb48_07307.pdf

56. يملك ذلك التلاعب كله إمكان كامنة بإحداث ضرر أكبر بواسطة الإنترنت؛ لأن تركيبة مجتمعنا بحد ذاتها تتحكم بها الشركات. كتب البروفســور ريتشــارد ليســيغ، وهو أســتاذ قانون في «جامعة هارفرد» عن بنية الحوســبة بوصفها أداة للســيطرة. لورانس ليســيغ (2006). كتاب: **الشــيفرة: القوانين الأخرى للفضاء السبراني، نسخة 2.0**. دار «بازيك بوكس».
http://codev2.cc

57. إد بلنكينغتون وآماندا ميشــيل (17 فبراير 2012)، صحيفة الغارديان، «أوباما و«فيســبوك» وقوة الصداقة: البيانات في حملة 2012 الانتخابيّة».
Guardian,
http://www.theguardian.com/world/2012/feb/17/obama-digital-data-machinefacebook-election

تانزينا فيغا (20 فبراير 2012)، صحيفة نيويورك تايمس، «بيانات شــبكيّة ســاعدت في توجيه الإعلانات في حملة 2012 الانتخابيّة».
New York Times,
http://www.nytimes.com/2012/02/21/us/politics/campaigns-use-microtargeting-to-attract-supporters.html

ناثان آبز (أكتوبر 2012). «تأثير «البيانات الضخمة» في مآل الحملات السياسيّة: الإعلان السياسي الموجّه إلى مجموعات ميكرويّة في انتخابات الرئاسة للعام 2012».

Interactive Advertising Bureau,
http://www.iab.net/media/file/Innovations_In_Web_Marketing_and_Advertising_delivery.pdf

58. ساشا آيزنبرغ (19 ديسمبر 2012). موقع «إم آي تي تكنولوجي ريفيو»، مقال: «كيف استعملت حملة الرئيس أوباما «البيانات الضخمة» في تعبئة الناخب الفرد».

MIT Technology Review,
http://www.technologyreview.com/featuredstory/509026/how-obamas-team-used-big-data-to-rally-voters

59. ميكاه آلتمان وكارين ماكدونالد وميتشل ماكدونالد (2005). «من يعيدون تقسيم المناطق الانتخابية بكبسة زر: كيف غيّرت الحوسبة إعادة ترسيم المقاطعات». من كتاب: **في الخطوط الحزبيّة: المنافسة، المحازبة وإعادة ترسيم المقاطعات في انتخابات الكونغرس**، تأليف: توماس إي. مان وبروس إي. كاين. «مطابع مؤسسات بروكينغز».

http://openscholar.mit.edu/sites/default/files/dept/files/pushbutton.pdf

ترايسي يان (23 يناير 2013)، صحيفة **بوسطن غلوب**، مقال: «تحويل الخريطة السياسيّة سلاحاً حزبيّاً».
Boston Globe,
http://www.bostonglobe.com/news/nation/2013/06/22/new-district-maps-reaped-rewards-for-gop-congress-butcost-fewer-moderates-more-gridlock/B6jCugm94tpBvVu77ay0wJ/story.html

60. آرش بدينفتون (9 أكتوبر 2013). مؤسّسة «فريدوم هاوس». مقال: «لتجديد الديمقراطيّة الأميركيّة، أزيلوا إعادة تخطيط المناطق الانتخابيّة».

Freedom House,
http://www.freedomhouse.org/blog/renew-american-democracy-eliminate-gerrymandering

برس ميلان (20 يوليو 2014). صحيفة **نيوز أوبزرفر**. مقال: «إعادة تخطيط المناطق الانتخابيّة في «نورث كارولينا» خسارة للديمقراطيّة».

http://www.newsobserver.com/2014/07/20/4014754/with-nc-gerrymandering-democracy.html

61. جون ماركوف (16 فبراير 1995). صحيفة **نيويورك تايمس**. مقال: «القبض على اللص السيبراني الأكثر خطورة في دواخل شبكته الخاصة».

New York Times,
http://www.nytimes.com/1995/02/16/us/a-most-wanted-cyberthief-is-caught-in-his-own-web.html

62. روبرت أوهارو جونيور (17 فبراير 2005). صحيفة **واشنطن بوست**. مقال: «السطو على هويات في شركة».
Washington Post,
http://www.washingtonpost.com/wp-dyn/articles/A30897-2005Feb16.html

63. براين كريبس (2 سبتمبر 2014). موقع «كريبس أون سيكيوريتي». مقال: «بنوك: السطو على بطاقات ائتمان في «هوم ديبو»».

Krebs on Security,
http://krebsonsecurity.com/2014/09/banks-credit-card-breach-at-home-depot.

64. دومينيك روش (3 أكتوبر 2014). صحيفة **الغارديان**. مقال: «بنك «جي بي مورغان» يكشف عملية اختراق كبرى لبياناته، تؤثر في 76 مليون أسرة».

Guardian,
http://www.theguardian.com/business/2014/oct/02/jp-morgan-76m-households-affected-data-breach

65. براين كريبس (20 أكتوبر 2013)، موقع «كريبس أون سيكيوريتي». مقال: «شركة «إيكسبيريان» باعت بيانات هويّات، استخدمت في سرقة».

Krebs on Security,
http://krebsonsecurity.com/2013/10/experian-sold-consumer-data-to-id-theft-service.

.66 م. ي. كاباي (2008). كتاب: **موجز لتاريخ جريمة الكومبيوتر: مقدّمة للطلبة**. جامعة نورويتش.
http://www.mekabay.com/overviews/history.pdf.

.67 أضحت تلك الظاهرة مشـكلة كبرى في الولايات المتحدة. مايكل كرانيش (16 فبراير 2014)، صحيفة **بوسطن غلوب**. مقال: «باتت «دائرة المداخيل الداخلية» مثقلة بجرائم سرقة الهويّة».
Boston Globe,
http://www.bostonglobe.com/news/nation/2014/02/16/identity-theft-taxpayer-information-major-problem-for-irs/7SC0BarZMDvy07bbhDXwvN/story.html.
SteveKroft (21 Sep 2014)

.68 في العـام 2014، عرفنـا أنّ «هاكـرز» صينيّين اخترقوا قاعدة بيانات تحتوي أسـماء حملـة الأذونات الأمنيّة في أميركا. لا نعلم إن كانوا يبحثون عن معلومات تسـاعدهم على ارتكاب جرائم، أم إنهم موظّفون في الاستخبارات الحكوميّـة يهدفـون للضغط على أشـخاص في مواقع نافذة. مايكل س. شـميدت وديفيد ي. سـانغر ونيكول بيلروث (9 يوليو 2014). صحيفة **نيويورك تايمس**. «»هاكرز» صينيّون يسـعون خلف معلومات أساسـيّة عن موظّفين أميركيّين».
New York Times,
http://www.nytimes.com/2014/07/10/world/asia/chinese-hackers-pursue-key-data-on-us-workers.html.

.69 لنعـط مجـرد نموذج عن ذلك. أصاب برنامج خبيث الحواسـيب في ما يزيد عـلى 1000 شركة في العام 2014، وسطا على أرقام حسابات بنكيّة. لم تعرف شركات كثيرة أنّها كانت من الضحايا.
نيكـول بيلروث (8 سـبتمبر 2014). صحيفـة **نيويورك تايمس**. مقـال: «اختراق بيانات «هـوم ديبو» ربما الأضخم حتى الآن».
New York Times,
http://bits.blogs.nytimes.com/2014/09/08/home-depot-confirms-that-it-was-hacked

.70 ريتشـارد وينتون (1 سبتمبر 2011). صحيفة **لوس أنجلوس تايمس**. مقال: «»الابتزاز الجنسي»: السجن 6 سنوات للـ«هاكر» الذي أوقع بالنساء والفتيات».
Los Angeles Times,
http://latimesblogs.latimes.com/lanow/2011/09/sextortion-six-years-for-oc-hacker-whoforced-women-to-give-up-naked-pics-.html.

.71 نايت أندرسـون (10 مارس 2013) موقع «آرس تكنيكا». مقال: «مقابلة مع الرجل الذي تجسّـس على نسـاء بواسطة كاميراتهن الشبكيّة».
Ars Technica,
http://arstechnica.com/tech-policy/2013/03/rat-breeders-meet-the-men-who-spy-on-women-through-their-webcams.

.72 كشـمير هيل (25 سـبتمبر 2012). مجلة **فوربس**. مقـال: «تفيد «لجنة التجارة الفيدراليّـة» أنّ شركات بيع حواسيب بالتقسيط التقطت صوراً لأزواج أثناء ممارسة الجنس».
Forbes,
http://www.forbes.com/sites/kashmirhill/2012/09/25/ftc-its-not-cool-to-put-spyware-on-rent-to-own-computers-without-customer-consent
دارا كير (22 أكتوبر 2013). شبكة «سي نت». مقال: «تسوية قضية شركة «آرون» لبيع الحواسيب بالتقسيط، مع «لجنة التجارة الفيدراليّة» بشأن التجسّس».
CNET,
http://www.cnet.com/news/aarons-computer-rental-chain-settles-ftc-spying-charges

الفصل 9: التنافسية التجارية

1. يـورد الكتـاب أن حقوقه تعود إلى العـام 1994، لكنه طُبِعَ في أكتوبر 1993. بروس شـناير (1994)، كتاب: **التشفير التطبيقي: بروتوكولات العمل، والخوارزميّات، وشيفرة المصدر في برنامج «سي»**.
https://www.schneier.com/book-applied.html

2. مجلة وايرد (أبريل 1996). مقال: «في الأكشاك الآن: كاتالوغ التشفير».
Wired,
http://archive.wired.com/wired/archive/4.04/updata.html.

3. سـتيفن ت. وولكـر (12 أكتوبر 1993). «شـهادة شـفويّة مـن سـتيفن ت. وولكر، رئيس شركة «تراسـتد إنفورمايشن سيستمز»، أمام «لجنة العلاقات الخارجية» في مجلس النواب».
http://fas.org/irp/congress/1993_hr/931012_walker_oral.htm.

4. في ما يلي بعض المصادر عن قصص رعب مماثلة ما زالت جارية. آلين ناكاشـيما (26 يوليو 2014). صحيفة واشنطن بوست. مقال: «تكاثر خدمات الاتّصال الجديدة بواسطة الإنترنت، يعيق عمل قوى إنفاذ القانون».
Washington Post,
http://www.washingtonpost.com/world/national-security/proliferation-of-new-online-communications-services-poses-hurdles-for-law-enforcement/2014/07/25/645b13aa-0d21-11e4-b8e5-d0de80767fc2_story.html.
أورين كير (19 سبتمبر 2014). صحيفة **واشنطن بوست**. مقال: «لعبة «آبل» الخطيرة».
Washington Post,
http://www.washingtonpost.com/news/volokh-conspiracy/wp/2014/
برنت كيندال (25 سبتمبر 2014). صحيفة **وول ستريت جورنال**. مقال: «مدير الـ«إف بي آي» يثير مخاوف بشأن الهواتف الذكيّة».
Wall Street Journal,
http://online.wsj.com/articles/fbi-director-raises-concerns-about-smartphone-security-plans-1411671434

5. صـاغ لويس فرييه، مدير الـ«إف بي آي» المسـألة على النحو التالي: «نحن نؤيّد التشـفير القوي المتماسـك. إذ تحتاجـه البلاد وصناعتها. كل ما نريده هو مجرد وجـود باب مصيدة يكون مفتاحه بيد قاضٍ، فندخل منه في حـال خطّط أحدهم جريمة». وظهر اقتباس مماثل من مستشـار الـ«إف بي آي» في الفصل 6من هذا الكتاب. بروك ن. مييكس (12 مايو 1995). «الاقتحام من باب المخدرات والإرهاب في التشفير».
http://www.cyberwire.com/cwd/cwd.95.05.12a.html

6. واين مادسن (نوفمبر 1994). «إشكاليّة الـ«كليبر»».
http://www.sciencedirect.com/science/article/pii/1353485894900973.
مات بليز (9 ديسمبر 2011). «مفتاح المتعهد من مسافة آمنة: استعادة لتجربة «كليبر شيب»».
http://www.crypto.com/papers/escrow-acsac11.pdf

7. امتلك الجيش الأميركي شـيئاً مُشـابِهاً من صنع «وكالة الأمن القومي» منذ 1987، حمل اسم «إس تي يو3-». «مؤسّسة الأمن العسكري» (فبراير 1997). «كتيب «إس تي يو- 3».
http://www.tscm.com/STUIIIhandbook.html

8. هال أبلسون وآخرون (يونيو 1999). مقال: «مخاطر استعادة المفتاح، مفتاح المتعهد والتشفير الموثوق من طرف ثالث».
https://www.schneier.com/paper-key-escrow.html

9. «متحف كريبتو» (2014). «المشفّر «تي أس دي- 3600-إي» من «إيه تي أند تي»».
http://www.cryptomuseum.com/crypto/att/tsd3600

10. دوروثي ي. كيننغ ودينس ك. برانشتاد (مارس 1996). «تصنيف نُظُم التشفير مع مفتاح المتعهد».
http://faculty.nps.edu/dedennin/publications/Taxonomy-CACM.pdf

11. لورانـس هوفمـان (10 يونيـو 1999). «التطوير المتواصل لمنتجات بتشـفير قوي ينافـس القوانين الأميركيّة للتصدير».
http://cryptome.org/cpi-survey.htm

12. يصف المقال التالي تلك الأزمنة. ستيفن ليفي (مايو 1993). مجلة وايرد. مقال: «متمردو التشفير».
Wired,
http://archive.wired.com/wired/archive/1.02/crypto.rebels_pr.html.

13. ناقـش المقال التالي الملامح الثلاثة لتلك الخسـائر. دانيـال كاهيل (29 يوليو 2014). «خسـائر الرقابة: تأثير «وكالة الأمن القومي» في الاقتصاد، حرية الإنترنت والفضاء السبراني».
http://www.newamerica.net/publications/policy/surveillance_costs_the_nsas_impact_on_the_economy_internet_freedom_cybersecurity

14. بارتون غيلمان ولورا بوارتراس (7 يونيو 2013). صحيفة واشنطن بوست. مقال: «الاستخبارات البريطانيّة والأميركيّة تنقّب في بيانات 9 شركات أميركيّة، ضمن برنامج سريّ واسع».
Washington Post,
http://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html

15. ديفيد جلبرت (4 يوليو 2013). مجلة انترناشـيونال بيزنس تايمس. مقال: «بعد الكشـوفات عن تجسّـس «وكالة الأمن القومي»، الشركات تتجه إلى سويسرا لتخزين بيانات «حوسبة السحاب»».
International Business Times,
http://www.ibtimes.co.uk/business-turns-away-dropbox-towards-switzerland-nsa-486613.

16. إلين ميسـمير (8 يناير 2014). مقال: «فضيحة «وكالة الأمن القومـي» تطارد شركات المعلوماتية والاتصالات في بريطانيا وكندا».
http://www.networkworld.com/article/2173190/security/nsa-scandal-spooking-it-pros-in-uk--canada.html.

17. شركة «إن تي تي كوميونيكاشنز» (28 مارس 2014). تقرير: «صدمات ما بعد «وكالة الأمن القومي»: سنودن غيّر مقاربة صُنّاع القرار في شركات المعلوماتية والاتصالات، لموضوع «حوسبة السحاب»».
http://nsaaftershocks.com/wp-content/themes/nsa/images/NTTC_Report_WEB.pdf

18. دانيال كاسترو (5 أغسطس 2013). «مؤسّسة الابتكار وتقنيّة المعلومات». دراسة: «كم يكلّف برنامج «بريزم» شركات «حوسبة السحاب» الأميركيّة»؟
Information Technology and Innovation Foundation,
http://www.itif.org/publications/how-much-will-prism-costus-cloud-computing-industry

أندريا بيترسون (7 أغسطس 2013). صحيفة واشنطن بوست. مقال: «تجسّس «وكالة الأمن القومي» يكلف شركات التكنولوجيا الأميركيّة 35 بليون دولار في 3 سنوات».
Washington Post,
http://www.washingtonpost.com/blogs/the-switch/wp/2013/08/07/nsa-snooping-could-costu-s-tech-companies-35-billion-over-three-years.

19. جيمس سـتاتن (14 أغسـطس 2013). مُدوّنة إلكترونيّة. مقال: «خسـائر برنامج «بريزم» ستفوق التوقّعات المتداولة».
James Staten's Blog,
http://blogs.forrester.com/james_staten/13-08-14-the_cost_of_prism_will_be_larger_than_itif_projects

20. كريسـتوفر ميامز (14 نوفمبر 2013). مقال: «خسائر «سيسكو» الفصليّة الموجعة توضح أن تجسّس «وكالة الأمن القومي» يمكنه أن يبعد الشركات الأميركيّة عن سوق بقرابة تريليون دولار».
http://qz.com/147313/ciscos-disastrous-quarter-shows-how-nsa-spying-could-freezeus-companies-out-of-a-trillion-dollar-opportunity

21. أنطون توريانوفسـكي وتوماس غريتا وسـام شوشـنر (30 أكتوبر 2013). صحيفة وول ستريت جورنال. مقال: «فضيحة «وكالة الأمن القومي» تخنق شركة «إيه تي أند تي»».

Wall Street Journal,
http://online.wsj.com/news/articles/SB10001424052702304073204579167873091999730

22. وولـف ريشــتر (17 أكتوبر 2013). مقال: «الكشـوفات عن «وكالة الأمن القومي» تقتـل المبيعات الإلكترونيّة لشركة «آي بي أم» في الصين».
http://www.testosteronepit.com/home/2013/10/17/nsa-revelations-kill-ibm-hardware-sales-in-china.html

23. سـبنسر ي. آنتـي (22 نوفمبر 2013). صحيفة وول سـتريت جورنـال. مقال: «مديـر «كوالكوم» يورد أن فضيحة «وكالة الأمن القومي» تؤثّر في أعمال شركته في الصين».
Wall Street Journal,
http://online.wsj.com/news/articles/SB10001424052702304337404579214353783842062

24. مارك سكوت (26 يونيو 2014). صحيفة نيويورك تايمس. مقال: «متأثّرة بفضيحة «وكالة الأمن القومي»، ألمانيا تلغي عقداً ضخماً مع «فيريزون» الأميركيّة».
New York Times,
http://www.nytimes.com/2014/06/27/business/angered-by-nsa-activities-germany-cancels-verizon-contract.html

25. سـتيفن كارتر (13 فبراير 2014). شـبكة «بلومبرغ نيوز» التلفزيونيّة. مقـال: «فجوة الثقة المكلفة للشركات الأميركيّة».
Bloomberg BusinessWeek,
http://www.businessweek.com/articles/2014-02-13/nsasnooping-backlash-could-cost-u-dot-s-dot-tech-companies-billions.
كلير كاين ميللر (22 مارس 2014). صحيفة نيويورك تايمس. مقال: «تجسّس «وكالة الأمن القومي» يلقي بتكاليف ضخمة على شركات المعلوماتية الأميركيّة».
New York Times,
http://www.nytimes.com/2014/03/22/business/fallout-from-snowden-hurtingbottom-line-of-tech-companies.html.

26. آشلي لو (18 مايو 2014). وكالة «رويترز» للأنباء. مقال: «جون تشامبرز يحض إدارة أوباما على كبح تجسّس «وكالة الأمن القومي»».
Reuters,
http://www.reuters.com/article/2014/05/18/cisco-systems-nsa-idUSL1N0O40F420140518

27. شون كالامار (14 مايو 2014). موقع «آرس تكنيكا». مقال: «صور مصنع «الترقية» لـ«وكالة الأمن القومي» تظهر زرع مكوّنات في محوّلات شركة «سيسكو»».
http://arstechnica.com/tech-policy/2014/05/photos-of-an-nsa-upgrade-factory-show-ciscorouter-getting-implant

28. دومينيـك روش (11 سـبتمبر 2013). صحيفـة الغارديان. مقـال: «زوكربرغ يعتـبر أن الحكومة الأميركيّة «حطّمت الأمور» بتصريحاتها عن «وكالة الأمن القومي»».
Guardian,
http://www.theguardian.com/technology/2013/sep/11/yahoo-ceo-mayer-jail-nsa-surveillance

29. كورنيليس راهن (13 سـبتمبر 2011). تلفزيون «بلومبرغ». مقال: «تطلب «دويتشـه تليكوم» صنع «سحابة ألمانيّة» لتبقي بياناتها بعيداً عن الولايات المتحدة».
Bloomberg News,
http://www.bloomberg.com/news/2011-09-13/deutsche-telekom-wants-german-cloud-toshield-data-from-u-s-.html.

30. آليسون غراند (20 نوفمبر 2013). مقال: «وفق المحاكم، تنتهك سياسات «غوغل» قوانين ألمانيا في الخصوصيّة».
http://www.law360.com/articles/490316/google-s-policies-violate-german-privacy-law-court-says

31. لويك إيسر (18 فبراير 2014). مقال: «وفق المحاكم، يجب على «فيسبوك» الانصياع لقوانين ألمانيا في حماية البيانات».
http://www.pcworld.com/article/2098720/facebook-must-comply-with-german-data-protection-law-court-rules.html

32. لويك إيسر (7 مايو 2013). مقال: «وفق المحاكم، تتعارض قواعد «آبل» في الخصوصيّة مع قوانين ألمانيا في حماية البيانات».
http://www.macworld.com/article/2038070/apples-privacy-policy-violates-german-data-protection-law-berlin-court-rules.html.

33. صحيفة دير شبيغيل (5 أغسطس 2013). مقال: «ارتدادات فضيحة «وكالة الأمن القومي»: وزير ألماني يروج لحظر الشركات الأميركيّة».
Der Spiegel,
http://www.spiegel.de/international/business/german-minister-on-eu-company-ban-for-privacy-violation-a-914824.html.

34. كريستا هاغز (27 مارس 2014). وكالة «رويترز». مقال: «خصوصيّة البيانات ترسم الجيل الجديد من حواجز التجارة الدوليّة».
Reuters,
http://www.reuters.com/article/2014/03/27/us-usa-trade-tech-analysis-idUSBREA2Q1K120140327

35. يقلق مديرون لشركات أميركيّة من ممارسة الحمائيّة ضد شركاتهم. ستيفن لاوسون (8 أكتوبر 2014). مقال: «تحذير من مديرين تنفيذيّين: النفور من الرقابة الأميركيّة يمكنه تحطيم الإنترنت».
http://www.itworld.com/security/440886/jitters-over-us-surveillance-could-break-internet-tech-leaders-warn

36. جيور ماسكولو وبن سكوت (أكتوبر 2013). مقال: «دروس من صيف سنودن: الطريق الصعب لاستعادة الثقة».
http://www.newamerica.net/sites/newamerica.net/files/policydocs/NAF-OTI-WC-SummerOfSnowdenPaper.pdf.
مارك سكوت (11 يونيو 2014). صحيفة نيويورك تايمس. مقال: «شركات أوروبيّة تجعل الخصوصيّة أداة ترويج لمبيعاتها».
New York Times,
http://bits.blogs.nytimes.com/2014/06/11/european-firms-turn-privacy-into-sales-pitch

37. تمنح شركة «بروتون مايل» السويسريّة بريداً إلكترونيّاً لا تطاله يد «وكالة الأمن القومي». جون بيغز (23 يونيو 2014). مقال: «شركة «بروتون مايل» السويسريّة تقدم خدمة بريد إلكتروني لا يشي بك إلى «وكالة الأمن القومي»».
http://techcrunch.com/2014/06/23/protonmail-is-a-swiss-secure-mailprovider-that-wont-give-you-up-to-the-nsa

38. جوناثان بالمار وجوزيف بايلي وسامر فرج (مارس 2000). دراسة: «دور الوسطاء في تطوير الثقة على الإنترنت: صعود الأطراف الثالثة الموثوقة ونصوص الخصوصيّة».
http://onlinelibrary.wiley.com/doi/10.1111/j.1083-6101.2000.tb00342.x/full.

39. يانيس تزاي وآخرون (يونيو 2007). دراسة: «تأثير الخصوصيّة الإلكترونيّة في سلوكيات التسوّق: دراسة تجريبيّة».
http://weis2007.econinfosec.org/papers/57.pdf

40. كادي تومبسـون (7 مارس 2014). شـبكة «آن بـي سي نيوز». مقال: «أترغـب في الخصوصيّة على الإنترنت؟ الشركات الجديدة تراهن أن المستخدمين مستعدون للدفع».
NBC News,
http://www.nbcnews.com/tech/security/want-privacy-online-start-ups-bet-users-are-ready-pay-n47186

41. «داك داك غو».
http://www.duckduckgo.com.

42. شارون بروفيس (26 سبتمبر 2014). موقع «سي نت». مقال: «10 أشياء يجب أن تعرفها عن «إيللو»: الشبكة الاجتماعيّة الخالية من الإعلانات».
CNET,
http://www.cnet.com/how-to/what-is-ello-thead-free-social-network.

الفصل 10: الخصوصيّة

1. في مـا يـلي مقال يرجع إلى العام 1979، يتحدّث عن الخصوصيّة كوسـيلة لإخفاء الشـخص حقائق عنه توخياً لتضخيم سمعته. ريتشارد بوزنر (1979). مقال: «الخصوصيّة، السريّة والسمعة».
http://chicagounbound.uchicago.edu/cgi/viewcontent.cgi?article=2832&context=journal_articles

2. دأب دانيال سـولوف عـلى التصدي لمقولة «لا شيء لإخفائه». دانيال ج. سـولوف (نوفمبر/ ديسـمبر 2007). مقال: ««ليس لديّ ما أخفيه»، والمفاهيم المغلوطة الأخرى عن الخصوصيّة».
http://papers.ssrn.com/sol3/papers.cfm?abstract_id=998565
دانيال ج. سولوف (15 مايو 2011). مقال: «لماذا الخصوصيّة تكون مهمّة حتى لو لم يكن لديك ما تخفيه».
https://chronicle.com/article/Why-Privacy-Matters-Even-if/127461.

3. صحيفة هافنغتون بوست (25 مايو 2011). مقال: «المدير التنفيذي لـ«غوغل» إريك شميدت يقول: إذا كان لديك ما لا تريد أي شخص آخر أن يعرفه، فلربما يجب عليك في المقام الأول ألا تفعل ذلك».
Huffington Post,
http://www.huffingtonpost.com/2009/12/07/google-ceo-on-privacy-if_n_383105.html

4. إلينور سميث (14 يوليو 2005). مقال: ««غوغل» يوازن بين الخصوصيّة والذيوع».
http://news.cnet.com/Google-balances-privacy,-reach/2100-1032_3-5787483.html.
راندال سـتروس (28 أغسـطس 2005). صحيفة نيويورك تايمس. مقال: «البحث عن أي شيء على «غوغل»، طالما أنّه ليس «غوغل» نفسه».
New York Times,
http://www.nytimes.com/2005/08/28/technology/28digi.html

5. بوبـي جونسـون (10 ينايـر 2010). صحيفة الغارديان. مقـال: «الخصوصيّة لم تعد عرفـاً اجتماعيّاً، وفق مؤسّس «فيسبوك»».
Guardian,
http://www.theguardian.com/technology/2010/jan/11/facebook-privacy

6. برايان بايلي (11 أكتوبر 2013). مقال: «زوكربرغ يشتري أربعة منازل قرب مسكنه في «بالو آلتو»».
http://www.mercurynews.com/business/ci_24285169/mark-zuckerberg-buys-four-houses-near-his-palo-altohome.

7. بيتر ي. ساند (ربيع/صيف 2006). مقال: «قيمة الخصوصيّة».
http://moritzlaw.osu.edu/students/groups/is/files/2012/02/5-Sand.pdf.

8. جوديث دونات (2014). «مطبعة معهد ماساشوستس للتقنية». كتاب: **الآلة الاجتماعيّة: تصاميم من أجل العيش على الإنترنت.**
MIT Press,
https://encrypted.google.com?id=XcgmnwEACAAJ

9. ديفيد كيركباتريك (2010). «دار سايمون أند شوستر». كتاب: **تأثير «فيسبوك»: القصّة الداخليّة للشركة التي تربط العالم.**
https://www.facebook.com/thefacebookeffect

10. يعرّف إيبين موغلِن الخصوصيّة في ثلاثة مكوّنات: «الأول هو السريّة بمعنى قدرتنا على الحفاظ على محتوى رسائلنا فلا يعرفها سوى من نقصد إرسالها لهم. الثاني هو إغفال الهويّة بمعنى سرية من يرسل الرسائل ومن يتلقاها، عندما يتعذّر الحفاظ على محتوى الرسائل. من الأهمية بمكان أن نحظى بإمكان إغفال الهويّة في ما ننشره ونقرؤه. الثالث هو الاستقلاليّة الذاتيّة، بمعنى قدراتنا على اتّخاذ القرارات المتعلّقة بحياتنا، بعيداً عن أي قوة تسعى لانتهاك سريّتنا أو إغفالنا الهويّة». إيبين موغلِن (27 مايو 2014). صحيفة **الغارديان**. مقال: «الخصوصيّة تتعرّض للهجوم: وثائق «وكالة الأمن القومي» تكشف تهديدات جديدة للديمقراطيّة».
Guardian,
http://www.theguardian.com/technology/2014/may/27/-sp-privacy-under-attack-nsa-files-revealed-new-threatsdemocracy.
ويقسّم دانيال ج. سولوف أستاذ القانون في «جامعة جورج واشنطن» الخصوصيّة إلى 6 أقسام: «1- الحق في أن نترك لشأننا. 2- تقييد وصول الآخرين إلى ذاتنا. 3- السريّة. 4- السيطرة على المعلومات الشخصيّة. 5- امتلاك النفس. و6- الحميميّة».
Daniel J. Solove (Jul 2002), «Conceptualizing privacy,» *California Law Review* 90,
http://scholarship.law.berkeley.edu/cgi/viewcontent.cgi?article=1408&context=californialawreview

11. دانا بويد (2014). «مطبعة جامعة يال». كتاب: **معقّدة: الحياة الاجتماعيّة للمراهقين المتّصلين شبكيّاً.**
http://www.danah.org/books/ItsComplicated.pdf.

12. اختُبِرَت تلك اليوتوبيا المعكوسة في الأدب وأخيلته. دايف إيغرز (2013). رواية: **الدائرة.**
http://www.mcsweeneys.net/articles/a-brief-q-a-withdave-eggers-about-his-new-novel-the-circle

13. هيلين نسينباوم (خريف 2011). دراسة: «مقاربة سياقيّة للخصوصيّة على الإنترنت».
http://www.amacad.org/publications/daedalus/11_fall_nissenbaum.pdf
آليكس مادريغال (29 مارس 2012). مجلة **آتلانتيك**. مقال: «الفيلسوف الذي ترك بصماته على السياسة الجديدة لـ«لجنة التجارة الفيدرالية» بشأن الخصوصيّة».
Atlantic,
http://www.theatlantic.com/technology/print/2012/03/the-philosopher-whose-fingerprints-are-all-over-the-ftcs-new-approach-to-privacy/254365.

14. جورج بنيشاس (مايو 2014). بحث: «نظرية الانتهاك في الخصوصيّة».
http://link.springer.com/article/10.1007%2Fs11158-014-9240-3

15. بيتر كلوبفر ودانيال روبنشتاين (صيف 1977). بحث: «مفهوم الخصوصيّة وأسسه البيولوجيّة».
https://www.princeton.edu/~dir/pdf_dir/1977_Klopfer_Rubenstein_JSocIssues.pdf.

16. بيتر واتس (9 مايو 2014). بحث: «مجتمع الأرض المحروقة: دليل المفجّر الانتحاري إلى الخصوصيّة على الإنترنت».
http://www.rifters.com/real/shorts/TheScorchedEarthSociety-transcript.pdf.

17. سيدني جورار (ربيع 1966). بحث: «عن المناحي النفسيّة للخصوصيّة».
http://scholarship.law.duke.edu/cgi/viewcontent.cgi?article=3110&context=lcp.

18. جيمس وتمان (أبريل 2004). مقال: «نظرتان ثقافيتان غربيّتان إلى الخصوصيّة: الكرامة في مواجهة الحريّة».
http://www.yalelawjournal.org/article/the-two-western-cultures-of-privacy-dignity-versus-liberty.

19. مايكل لينش (22 أكتوبر 2013). صحيفة نيويورك تايمس. مقال: «الخصوصيّة وتهديد الذات».
http://opinionator.blogs.nytimes.com/2013/06/22/privacy-and-the-threat-to-the-self.

20. صودرت تلك الوثائق في سياق قضيّة «إيران- كونتراس». مايكل تاكيت (14 شباط 1987). صحيفة شيكاغو تريبيون. مقال: «سجلات الكومبيوتر تروي حكايات إيران: مواد مطبوعة بواسطة الكومبيوتر تدل المفتّشين على مذكّرات من رسميّين».
Chicago Tribune,
http://articles.chicagotribune.com/1987-02-14/news/8701120148_1_nsc-staff-professional-office-system-profs

21. إليزابيث وازرمان (17 نوفمبر 1998). شبكة «سي آن آن». مقال: «محفوظات غيتس تثير ضحك القضاة».
CNN,
http://edition.cnn.com/TECH/computing/9811/17/judgelaugh.ms.idg.

22. بيل هتشنسون (31 أغسطس 2014). صحيفة نيويورك دايلي نيوز. مقال: «جينيفر لورانس وممثلات أخريات، تسرّبت صورهن عاريات بعد فضيحة تسرب بيانات ضخمة».
New York Daily News,
http://www.nydailynews.com/entertainment/gossip/jennifer-lawrence-celebrities-nude-photos-leaked-internet-article-1.1923369

23. للغاية نفسها، تسوّق شركة «سيرفال بيومتريكس» ماسحات ضوئيّة لرخص قيادة المركبات. شركة «سيرفال بيومتريكس» (2014). منشور: «أمن النوادي: «ماسحات ضوئيّة لبطاقات الهويّة مخصّصة للبارات والنوادي الليليّة»».
http://www.servallbiometrics.com/index.php/products

24. (14 مايو 2007). مقال: «رسم المستقبل»، في مدوّنة «تشارلي دايري» الإلكترونيّة.
Charlie's Diary,
http://www.antipope.org/charlie/blog-static/2007/05/shaping_the_future.html.

25. هناك مقال قصير لتيد شيانغ يعالج ذلك الأمر، عنوانه «حقيقة الواقع، حقيقة المشاعر».
http://subterraneanpress.com/magazine/fall_2013/the_truth_of_fact_the_truth_of_feeling_by_ted_chiang.

26. كان الباحث في الاتصالات هارولد إيننيس سبّاقاً في وصف الافتراضات القبليّة الموجودة في أشكال الاتصالات المختلفة. ولاحظ أن بعض وسائط الاتّصالات تحفظ الاتّصال بالوقت، فيما تعمل وسائط أخرى بواسطة الأمكنة. هارولد إيننيس (1951)، كتاب: **الافتراض القبلي في الاتصال**. «مطبعة جامعة تورنتو».
http://books.google.com?id=egwZyS26booC

27. هناك بحوث أخّاذة في هذا الشأن. نحن ننسى تفاصيل حوادث مهمّة أيضاً. إذ درس بحّاثة ذكريات الناس عن أمكنة وجودهم أثناء مشاهدتهم انفجار مكوك الفضاء «تشالنجر»، والإعلان عن نتيجة محاكمة لاعب البيسبول الأسمر أو. جي. سيمبسون بقضية مقتل عشيقته، وتغطية ضربات الإرهاب في 9/11. جون نيل بوحنون الثالث (يوليو 1998)، مقال: «التماعات الذاكرة في تذكّر كارثة مكوك الفضاء: قصّة نظريّتين».
http://www.sciencedirect.com/science/article/pii/0010027788900364
أندرو أر. إيه. كونواي وآخرون (يوليو 2008). «التماعات الذاكرة عن حوادث 9/11».
http://onlinelibrary.wiley.com/doi/10.1002/acp.1497/abstract

28. متشيل ناتيفيداد رودريغز وموريس إمسيلم (مارس 2011). «مشروع القانون القومي للتوظيف». بحث: «65 مليوناً يجب ألا يتقدّموا للوظائف: نظرة إلى إعادة رسم الخلفيّة الجرميّة للمتقدّمين للوظائف».
National Employment Law Project,
http://www.nelp.org/page/-/65_Million_Need_Not_Apply.pdf.

29. ويندي هيو كيونغ شون (خريف 2008). مقال: «الزائل الصامد، أو الذاكرة هي المستقبل».
http://www.ucl.ac.uk/art-history/events/past-imperfect/chun-reading

30. بروس شناير (27 فبراير 2014). صحيفة الغارديان. مقال: «الروبوتات الافتراضيّة لـ«وكالة الأمن القومي» تعمل على «جمع» بياناتك، ولا يحاسبها أحد على ذلك».

Guardian,
http://www.theguardian.com/commentisfree/2014/feb/27/nsa-robots-algorithm-surveillance-bruce-schneier

31. «مؤسّسة الحدود الإلكترونيّة» (2013). وثيقة: «تلاعب الحكومة بالكلمات عند الحديث عن التجسّس المحلي لـ«وكالة الأمن القومي»».
https://www.eff.org/nsa-spying/wordgames
تيم تريفور (14 أغسطس 2013). «مؤسّسة الحدود الإلكترونيّة». بحث: «دليل إلى الخداع والتضليل والتلاعب بالكلمات، الذي يلجأ إليه الرسميّون لتضليل الجمهور عند حديثهم عن رقابة «وكالة الأمن القومي»».
Electronic Frontier Foundation,
https://www.eff.org/deeplinks/2013/08/guide-deceptions-word-games-obfuscations-officials-use-mislead-public-about-nsa

32. أورد دليل عن المهمّات صادر في 1982، أنّه: «... يجب أن يستخدم وصف «جمع» للمعلومات حصريّاً عندما يجري تلقّيها من موظّف في القسم الاستخباراتي من «وزارة الدفاع» بهدف الاستعمال، في سياق مهمّاته الرسميّة». وكذلك: «يستعمل وصف «جمع» للمعلومات التي تصل من الوسائط الإلكترونيّة، بصورة حصريّة عند تحويلها إلى شكل قابل للفهم». وزارة الدفاع الأميركيّة، مكتب نائب وزير الدفاع (ديسمبر 1982). فصل: «الإجراءات التي تتحكم بنشاطات الأقسام الاستخباراتيّة في وزارة الدفاع، عندما تكون مؤثّرة في الأشخاص في الولايات المتحدة».
DoD 5240-1R, p. 15,
http://www.fas.org/irp/doddir/dod/d5240_1_r.pdf.

33. تبدي وزارة الدفاع تحوّطات حتى ضد مجرد التفكير بالكلمات واستعمالها بشكل صحيح. «الإجراء 2 يقود قارئ المذكرة «5204.1 - آر» أثناء تعرّفه للمرّة الأولى إلى «متاهة» القوانين. للبدء بالرحلة، من الضروري التوقّف أولاً وضبط الألفاظ التي تستعملها. إن الكلمات والمصطلحات الواردة في المذكرة «-5204.1 آر» لها معانٍ محدّدة، ويحدث غالباً أن ينقاد البعض بعيداً عندما يعتمدون على المعنى الشائع أو المفهومي، لتعريف كلمة معيّنة».
US Defense Intelligence Agency, Defense HUMINT Service (Aug 2004), ***Intelligence Law Handbook***, Defense Intelligence Management Document CC-0000-181-95,
https://www.aclu.org/files/assets/eo12333/DIA/Intelligence%20Law%20Handbook%20Defense%20HUMINT%20Service.pdf.

34. آندريا ميتشيل (9 يونيو 2013). شبكة تلفزيون «آن بي سي». مقال: «مقتطفات من مقابلة آندريا ميتشيل مع جيمس كلابر، مدير الاستخبارات القوميّة».
NBC News,
http://www.nbcumv.com/mediavillage/networks/nbcnews/pressreleases?pr=contents/pressreleases/2013/06/09/nbcnewsexclusiv1370799482417.xml.

35. رون وايدن (12 مارس 2013). موقع «يوتيوب». «وايدن في جلسة الاستماع للاستخبارات عن الرقابة بالـ«جي بي أس» وجمع «وكالة الأمن القومي» البيانات».
YouTube,
https://www.youtube.com/watch?v=QwiUVUJmGjs.

36. «غوغل» (2014). «الإعلانات في «جي ميل»».
https://support.google.com/mail/answer/6603?hl=en

37. في 2010، طمأنتنا «وكالة أمن النقل» بأنّ أجهزة المسح الضوئي للجسد كاملاً، لا تخزّن معلومات. في ما بيّنت وثائق سُلّمت إلى «مركز معلومات الخصوصيّة الإلكترونيّة» أن تلك الماسحات تُشحَن مع أقراص صلبة ومنافذ لأدوات ذاكرة الـ«فلاش» من نوع «يو إس بي». غينغر ماككول (3 أغسطس 2010). تقرير: «وثائق تظهر أن ماسحات الأجساد ضوئيّاً تخزن البيانات روتينيّاً».
Electronic Privacy Information Center,
http://epic.org/press/EPIC_Body_Scanner_Press_Release_08_03_10.pdf.

Declan McCullagh (4 Aug 2010), «Feds admit storing checkpoint body scan images,» *CNET*,
http://www.cnet.com/news/feds-admit-storing-checkpoint-body-scan-images.

«إدارة وكالة أمن النقل» (6 أغسطس 2010). «المدوّنة الإلكترونيّة للوكالة». «رد «وكالة أمن النقل» على أسئلة السلطة الفيدرالية، يعترف بأن نقاط التفتيش تخزّن صوراً ضوئيّة للأجساد».
TSA Blog,
http://blog.tsa.gov/2010/08/tsa-response-to-feds-admit-storing.html

38. للسـبب عينه، لا نحتج على الدمى من نوع «فوربيز»، لكننا قد نحتج لو أنها تحتوي أدوات تسـجيل. ومع ذلك، أبدت «وكالة الأمن القومي» قلقها لبعض الوقت؛ بشأن ذلك الأمر. «هيئة الإذاعة البريطانيّة» (13 يناير 1999). «هل «فوربي» دمية أم جاسوس»؟
BBC News,
http://news.bbc.co.uk/2/hi/americas/254094.stm.

39. بروس شناير (21 أكتوبر 2013). مجلة آتلانتيك. مقال: «ليس منطقياً دفاع «وكالة الأمن القومي» عن الجمع المكثّف للبيانات».
Atlantic,
http://www.theatlantic.com/politics/archive/2013/10/why-the-nsas-defense-of-mass-data-collection-makes-nosense/280715.

40. بروس شناير (2000). كتاب أسرار وأكاذيب. دار «ويلي» للنشر.
http://www.wiley.com/WileyCDA/WileyTitle/productCd-0471453803.html.

41. تشـارلز غـلاسر (1 يونيـو 2011). «جامعة جـورج واشـنطن». دراسـة: «ردع الهجمات السـبرانيّة والأمن الاستراتيجي للولايات المتحدة».
Report GW-CSPRI-2011-5, George Washington University Cyber Security Policy and Research Institute,
http://www.cspri.seas.gwu.edu/uploads/2/1/3/2/21324690/2011-5_cyber_deterrence_and_security_glaser.pdf.

جوزيف س. ناي جونيور (مايو 2010). «كلية كنيدي في جامعة هارفرد». دراسة: «قوة الفضاء السبراني».
Harvard Kennedy School, Belfer Center for Science and International Affairs,
http://belfercenter.ksg.harvard.edu/files/cyber-power.pdf.

42. تشـارلز كلوفر (11 مارس 2009). صحيفة فاينْنشال تايمس. مقال: «مجموعة يساندها الكرملين مسؤولة عن الهجمات السبرانيّة على أستونيا».
Financial Times,
http://www.ft.com/cms/s/0/57536d5a-0ddc-11de-8ea3-0000779fd2ac.html

43. نيكول بيرلروث (31 يناير 2013). صحيفة نيويورك تايمس. مقال: «مجموعة «هاكرز» من الصين هاجمت نيويورك تايمس خلال الشهور الـ4 الماضية».
New York Times,
http://www.nytimes.com/2013/01/31/technology/chinese-hackers-infiltrate-new-york-times-computers.html.

44. ويليـام جي. برود، جون ماركوف وديفيد ي. سـانغر (15 ينايـر 2011). صحيفة نيويورك تايمس. مقال: «تجربة إسرائيليّة على دودة إلكترونيّة أدّت لتأخير في برنامج إيران النووي».
New York Times,
http://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html

ديفيد ي. سانغر (1 يونيو 2012). صحيفة نيويورك تايمس. مقال: «أوباما أمر بشن سلسلة غارات سبرانيّة ضد إيران».
New York Times,
http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html.

45. تقييد إغفال الهويّة لا يقضي على التصيّد. إذ إنّ سلوك الناس على الإنترنت معقّد، وهو أقرب إلى إرخاء القيود الاجتماعيّة منه إلى السعي لإغفال الهويّة. جون سولر (يونيو 2004). مقال: «التحلّل الاجتماعي في الفضاء الافتراضي».
http://online.liebertpub.com/doi/abs/10.1089/1094931041291295.

46. فيليب وينتر وستيفان ليندسكوك (6 أغسطس 2012). «منتدى «يوزنيكس». ورقة بحث: «كيف يعمل «جدار النار» الصيني العظيم على صد نظام «تور»».
USENIX Workshop on Free and Open Communications on the Internet, Bellevue, Washington, https://www.usenix.org/system/files/conference/foci12/foci12-final2.pdf

47. ليون بانيتا (11 أكتوبر 2012). وزارة الدفاع. «ملاحظات من وزير الدفاع ليون بانيتا حول الأمن السبراني، إلى المدراء التنفيذيّين للشركات المهتمين بالأمن القومي».
US Department of Defense,
http://www.defense.gov/transcripts/transcript.aspx?transcriptid=5136.

الفصل 11: الأمن

1. بروس شناير (17 مايو 2007). مجلة وايرد. مقال: «دروس من الهجوم في «جامعة فرجينيا»: المخاطر النادرة تولّد ردود أفعال لا عقلانيّة».
Wired,
http://archive.wired.com/politics/security/commentary/securitymatters/2007/05/securitymatters_0517

2. المدوّنة الإلكترونيّة لواشنطن (15 أغسطس 2014). مقال: «أنت معرّض للموت على يد شرطي بتسعة أضعاف موتك بيد إرهابي».
Washington's Blog,
http://www.washingtonsblog.com/2014/08/youre-nine-times-likely-killed-police-officer-terrorist.html

3. سبنسر إكرمان (13 ديسمبر 2013). صحيفة **الغارديان**. مقال: «تقارير تفيد بأن «وكالة الأمن القومي» تفكّر بعدم إحداث تغيير واسع في برامجها للتجسس».
Guardian,
http://www.theguardian.com/world/2013/dec/13/nsa-review-to-leave-spying-programs-largely-unchanged-reports-say.

4. عندما نسترجع حدثاً ما ونرى الأدلّة كلها، نعتقد غالباً بأنه كان واجباً علينا توصيل النقط. يملك ذلك الأمر اسماً: التحيّز بالاسترجاع. إذ تتوضّح الأجزاء المفيدة من البيانات بعد الواقعة، أما قبلها فلم تكن تلك الأجزاء سوى قسم يسير من ملايين البيانات العديمة الدلالة. وكذلك فمن الممكن تجميع تلك الأجزاء نفسها لتدل على مليون اتّجاه مختلف.

5. نيسم نيكولاس طالب (2007). «مغالطة السرد» في كتاب **البجعة السوداء: تأثير غير متوقّع تماماً**. دار «راندوم هاوس».
http://www.fooledbyrandomness.com.

6. وكالة أنباء «أسوشيتدبرس» (2 فبراير 2012). صحيفة **يو أس إيه توداي**. مقال: «القائمة الأميركيّة للممنوعين من السفر جوّاً تتضاعف في سنة واحدة».
USA Today,
http://usatoday30.usatoday.com/news/washington/story/2012-02-02/no-fly-list/52926968/1.

7. إريك شميدت ومايكل س. شميدت (24 أبريل 2013). صحيفة **نيويورك تايمس**. «وكالتان أميركيّتان وضعتا مفجّر ماراثون «بوسطن» على قوائمهما للمراقبة».

New York Times,
https://www.nytimes.com/2013/04/25/us/tamerlan-tsarnaev-bomb-suspect-was-on-watch-lists.html

8. ي. دبليو. تي نغاي وآخرون (فبراير 2011). دراسة: «تطبيق تقنية التنقيب في البيانات في تقصي تزوير بطاقات الائتمان: إطار أكاديمي للعمل ومراجعة للأدبيّات».

https://www.sciencedirect.com/science/article/pii/S0167923610001302

9. إيريكا هاريل ولين لانغتون (12 ديسمبر 2013). مكتب الإحصاءات في وزارة العدل. تقرير: «ضحايا سرقة الهويّة في 2012».

US Bureau of Justice Statistics,
http://www.bjs.gov/index.cfm?ty=pbdetail&iid=4821.

10. «مكتب الموثوقيّة الحكوميّة» (2013). تقرير: «التهرّب الضرائبي في الملاذات الآمنة: «وكالة المداخيل الدخليّة» تجمع بلايين الدولارات، لكن التهرّب الضرائبي مستمر».

Report GAO-13-318,
http://www.gao.gov/assets/660/653369.pdf

11. والتر بيري وآخرون (2013). «مؤسّسة راند». بحث: «شرطة توقّعيّة: دور توقّع الجرائم في عمليات إنفاذ القانون».

RAND Corporation,
https://www.ncjrs.gov/pdffiles1/nij/grants/243830.pdf.

12. جون مولر ومارك ستيوارت (2011). «مطبعة جامعة أوكسفورد». كتاب: **إرهاب، أمن ونقود: التوازن بين المخاطر والفوائد والتكاليف في وزارة الأمن الوطني**.

Oxford University Press, chap. 2,
http://books.google.com/books?id=jyYGL2jZBC4C

13. جيف جوناس وجيم هاربر (11 ديسمبر 2006). منشورات مؤسّسة «كاتو». «الكفاءة في محاربة الإرهاب والدور المحدود للتنقيب التوقّعي في البيانات».

Cato Institute,
http://www.cato.org/publications/policy-analysis/effective-counterterrorism-limited-role-predictive-data-mining.

فريد كايت (صيف 2008). جامعة هارفرد. دراسة: «التنقيب الحكومي في البيانات: الحاجة إلى إطار قانوني».
Harvard Civil Rights-Civil Liberties Law Review
43,
http://www.law.harvard.edu/students/orgs/crcl/vol43_2/435-490_Cate.pdf.

14. ج. ستيورات مندونهال ومارك شميدهوفر (شتاء 2012- 2013). دراسة: «اختبار انتقائي للإرهاب».
http://object.cato.org/sites/cato.org/files/serials/files/regulation/2013/1/v35n4-4.pdf

كوري شيفرز (6 يونيو 2013). مقال: «ما أرجحيّة أن يلتقط برنامج «بريزم» لـ«وكالة الأمن القومي» إرهابيّاً؟».

http://bayesianbiologist.com/2013/06/06/how-likely-is-the-nsaprism-program-to-catch-a-terrorist

مارسي ويلر (15 يونيو 2013). مقال: «انعدام كفاءة «الأخ الكبير»: الروابط ومصنع الإرهاب».
http://www.emptywheel.net/2013/06/15/the-inefficacy-of-big-brother-associations-and-the-terror-factory.

15. في علم الإحصاء، يسمّى ذلك «مغالطة المعدّل الأساسي»، وينطبق على حقول أخرى. ومثلاً، حتى أشد الفحوص الطبيّة دقّة تصبح أداة انتقاء مثيرة للإشكاليّات، عندما تكون نسبة المرض نادرة بين السكان. وتعمّدت ألا أناقش الرياضيّات التي تكمن خلف ذلك، لكن المهتمين يستطيعون قراءة تلك التفاصيل. جيف جوناس وجيم

هاربر (11 ديسمبر 2006). منشورات مؤسّسة «كاتو». «الكفاءة في محاربة الإرهاب والدور المحدود للتنقيب التوقّعي في البيانات».

Cato Institute,

http://www.cato.org/publications/policy-analysis/effective-counterterrorism-limited-role-predictive-data-mining

16. ج.د. توسيل (19 يونيو 2013). مقال: «لماذا نتجسّس على الجميع؟ لأنك تحتاج كومة القش كي تعثر على الإبرة».

Reason,

http://reason.com/blog/2013/07/19/why-spy-on-everybody-because-you-need-th

17. مايك مازنيك (15 أكتوبر 2013). موقع «تيك درت». مقال: «الوثائق الأخيرة عن «وكالة الأمن القومي» تظهر أن الإفراط في «تجميع القش» يصعّب عمل الوكالة».

Tech Dirt,

https://www.techdirt.com/articles/20131014/17303424880/latest-revelationsshow-how-collecting-all-haystacks-to-find-data-makes-nsas-job-harder.shtml

18. كريس يونغ (12 مارس 2012). مجلة فوربس. مقال: «إعادة تعريف الاستخبارات العسكريّة: «البيانات الضخمة» في أرض المعركة».

Forbes,

http://www.forbes.com/sites/techonomy/2012/03/12/military-intelligence-redefined-big-data-in-the-battlefield

برنامج «وكالة الأمن القومي» في التجسّس. مات بريغز (7 يونيو 2013). مدوّنة «مات بريغز». مقال: «التنقيب في البيانات: «بريزم»، «وكالة الأمن القومي» والإنذارات الكاذبة الإيجابيّة: تحديث».

William M. Briggs,

http://wmbriggs.com/blog/?p=8239

19. لويل بيرغمان وآخرون (17 يناير 2006). صحيفة نيويورك تايمس. مقال: «بيانات وكالة تجسّس بعد 11/9، أوصلت الـ«إف بي آي» إلى طرق مسدودة».

New York Times,

http://www.nytimes.com/2006/01/17/politics/17spy.html.

20. «مكتب الموثوقيّة الحكوميّة» (26 مارس 2013). تقرير: «المشاركة في المعلومات: خطوات إضافية مطلوبة لتدعيم المشاركة في التقارير عن النشاطات المشبوهة المتّصلة بالإرهاب».

Report GAO-13-233,

http://www.gao.gov/assets/660/652995.pdf.

21. يوشاي بنكلر (8 أكتوبر 2013). صحيفة الغارديان. مقال: «حقيقة: لا تحصل «وكالة الأمن القومي» إلا معلومات شحيحة من «ميتاداتا» الأميركيّين. لذا، فلنتوقف عن جمعها».

Guardian,

http://www.theguardian.com/commentisfree/2013/oct/08/nsa-bulk-metadata-surveillance-intelligence.

بيتر برغن (يناير 2014). مقال: «هل توقف برامج التجسّس المكثفة لـ«وكالة الأمن القومي» الإرهاب؟»

http://newamerica.net/publications/policy/do_nsas_bulk_surveillance_programs_stop_terrorists

22. مارسي ويلر (12 ديسمبر 2013). مقال: «هل قاضت وزارة العدل بسالي موالين لمجرد القول بنجاح «الفصل 15»؟»

http://www.emptywheel.net/2013/12/12/did-doj-prosecute-basaaly-moalin-just-to-have-asection-215-success

23. يقدّم أمن الطائرات أمثلة كثيرة. في 2001، وضع ريتشارد ريد قنبلة في حذائه، وكان الأثر المباشر لذلك أنه يجب علينا جميعاً خلع أحذيتنا في المطارات منذها.

24. فرانسيس غويّار (10 يونيو 2013). مجلة فورتشن. مقال: «لا تمثّل «البيانات الضخمة» المتأتيّة من تجسّس «وكالة الأمن القومي» حتى استراتيجيّة مجدية».

Fortune,

http://management.fortune.cnn.com/2013/06/10/bigdata-nsa-spying-is-not-even-an-effective-strategy

إد بلكينغتون ونيكولاس واط. (12 يونيو 2013). صحيفة الغارديان. مقال: «وفق خبراء، رقابة «وكالة الأمن القومي» لم تفسد سوى خطط إرهابيّة قليلة تماماً».

Guardian,

http://www.theguardian.com/world/2013/jun/12/nsa-surveillance-dataterror-attack

25. جيفري سايفرت (3 أبريل 2008). خدمة الكونغرس للبحوث. تقرير: «التنقيب في البيانات و«الأمن الوطني»: مراجعة عامة».

Congressional Research Service,

http://www.fas.org/sgp/crs/homesec/RL31798.pdf

26. بيتر بيرغن (30 ديسمبر 2013). شبكة «سي آن آن». مقال: «هل كان لرقابة «وكالة الأمن القومي» كشف مخططات 9/11؟»

CNN,

http://www.cnn.com/2013/12/30/opinion/bergen-nsa-surveillance-september-11

27. سايمون شوستر (19 أبريل 2013). مجلة تايم. مقال: «الإخوة تسارناييف: تلميحات إلى دوافع مفجّري «بوسطن»».

Time,

http://world.time.com/2013/04/19/the-brothers-tsarnaevs-motives.

28. مارسي ويلر (12 أبريل 2014). مقال: «بعد يوم من وضع كاتالوغات حكوميّة من البيانات التي جمعتها «وكالة الأمن القومي»، رفضت وزارة العدل إصدار مذكّرة إلى دزوخار [أحد مفجّري «بوسطن»]».

http://www.emptywheel.net/2014/04/12/the-day-after-governmentcatalogs-data-nsa-collected-on-tsarnaevs-doj-refuses-to-give-dzhokhar-notice

29. «اللجنة القوميّة عن هجمات الإرهاب» (2004). «تقرير لجنة 9/11: التقرير النهائي لـ«اللجنة القوميّة عن النشاطات الإرهابيّة ضد الولايات المتحدة».

http://www.gpo.gov/fdsys/pkg/GPO-911REPORT/pdf/GPO-911REPORT.pdf.

30. دان إيغين وكارين دي يونغ وسبنسر س. هسو (27 ديسمبر 2009). صحيفة واشنطن بوست. مقال: «المشتبه فيه في حادثة الطائرة كان مدرجاً في قاعدة بيانات عن الإرهاب، عقب تحذير والده رسميّين أميركيّين».

Washington Post,

http://www.washingtonpost.com/wp-dyn/content/article/2009/12/25/AR2009122501355.html.

31. دومينيك كاسكياني (7 سبتمبر 2009). «بي بي سي نيوز». مقال: «مخطط المتفجّرات السائلة: ما الذي حدث؟».

BBC News,

http://news.bbc.co.uk/2/hi/uk_news/8242479.stm

32. تفاخرت «وكالة الأمن القومي» بإحرازها 54 نجاحاً في مواجهة الإرهاب، لكن الرقم لم يصمد أمام التدقيق. لم تكن غالبية تلك الحالات مخططات إرهابيّة، ومعظمها كان خارج الولايات المتحدة. جوستان إليوت وثيودوريك ميار (11 سبتمبر 2013). موقع «بروبابليكا». مقال: «مزاعم بأن «وكالة الأمن القومي» «أحبطت مخطّطاً» تنتشر على الرغم من غياب الأدلة».

Pro Publica,

http://www.propublica.org/article/claim-on-attacks-thwarted-by-nsa-spreads-despitelack-of-evidence.

33. كيفن ستروم وجون هوليوود (2010). وزارة الأمن الوطني. مقال: «التأسيس على التلميحات: تقييم النجاح

والإخفاق في تقصي مخططات الإرهاب في الولايات المتحدة».
Institute for Homeland Security Solutions,
http://sites.duke.edu/ihss/files/2011/12/Building_on_Clues_Strom.pdf

34. بروس شناير (8 سبتمبر 2005). مجلة وايرد. مقال: «الإرهابيّون لا يصنعون مخططاتهم اقتباساً من الأفلام».
Wired,
http://archive.wired.com/politics/security/commentary/securitymatters/2005/09/68789

35. بروس شـنـايـر (2012). كتاب: كَذَبَة ومتمردون: تفعيل الثقة التي يحتاجها المجتمع لينمو. دار «ويلي» للنشر.
http://www.wiley.com/WileyCDA/WileyTitle/productCd-1118143302.html.

36. روس أندرسون (2 أكتوبر 2001). «جامعة كامبردج». دراسة: «صعوبة أمن البيانات: مقاربة اقتصاديّة».
University of Cambridge Computer Laboratory,
http://www.acsac.org/2001/papers/110

ماثيـو ميللر وجون بريككي غريغـوري كونتي (29 نوفمبر 2012). صحيفة الحروب الصغيرة. مقال: «لماذا يخطئ حدسك على الأرجح بشأن الأسلحة السبرانيّة؟».
Small Wars Journal,
http://smallwarsjournal.com/jrnl/art/why-your-intuitionabout-cyber-warfare-is-probably-wrong.

37. بـروس شـنـايـر (19 نوفمبر 1999). موقع «إنفورمايشـن سـكيوريتي». مقـال: «مرافعة لأجل البسـاطة: لا تستطيع حماية ما لا تفهمه».
Information Security,
https://www.schneier.com/essay-018.html

38. إدوارد توفت (2003). «منتدى إدوارد توفت». تقرير: «لماذا يصعب صنع برامج رقميّة جيّدة؟».
Edward Tufte Forum,
http://www.edwardtufte.com/bboard/qand-a-fetch-msg?msg_id=0000D8

جيمـس كـواك (8 أغسـطس 2012). صحيفة آتلانتيـك. مقال: «البرامـج الرقميّة تدير العالـم: ألا يجدر بنا التوجّس من ضعف غالبيتها؟».
Atlantic,
http://www.theatlantic.com/business/archive/2012/08/software-runs-the-world-how-scaredshould-we-be-that-so-much-of-it-is-so-bad/260846.

39. مايـكل رايلي (13 مـارس 2014). مجلة بلومبرغ بيزنيس ويك. مقال: «إنذارات مهملة، والاسـتيلاء على 40 مليون رقم لبطاقات ائتمان: كيف انفجرت مسألة «تارغت»؟».
Bloomberg Businessweek,
http://www.businessweek.com/articles/2014-03-13/target-missed-alarms-inepic-hack-of-credit-card-data.

40. إليزابيـث هاريس (17 يناير 2014). صحيفة نيويورك تايمس. مقـال: «ممر مريب إلى محافظ نقود زبائن «تارغت»».
New York Times,
http://www.nytimes.com/2014/01/18/business/a-sneaky-path-into-target-customers-wallets.html

41. إليزابيث هاريس (6 مايو 2014). صحيفة نيويورك تايمس. مقال: «اختراق «تارغت» يطيح برئيسها».
New York Times,
http://www.nytimes.com/2014/05/06/business/target-chief-executive-resigns.html

42. نيكـول برلروث (31 يناير 2013). صحيفة نيويورك تايمس. مقال: «مجموعة «هاكرز» من الصين هاجمت نيويورك تايمس خلال الشهور الـ4 الماضية».
New York Times,

http://www.nytimes.com/2013/01/31/technology/chinese-hackers-infiltrate-new-york-times-computers.html.

43. يتمثّل هدفها حاضراً في الوصول إلى سرعات في الحوسبة تقاس بالـ«إكزا فلوب» [إكزا= بليون بليون، والـ«فلوب» تعبير يعني «عملية طافية» وهو وصف لتناقل المعلومات في ذاكرة الكومبيوتر]، ما يساوي كوينتليون [= واحد وإلى جانبه 18 صفراً] عملية في الثانية. جيمس بامفورد (15 مارس 2012)، مجلة وايرد، مقال: «وكالة الأمن القومي تبني المركز الأضخم للتجسّس في البلاد (راقب ما تقوله)».

Wired,

http://www.wired.com/threatlevel/2012/03/ff_nsadatacenter/all

44. بروس شناير (4 أكتوبر 2013). صحيفة الغارديان. مقال: «الجهوم على برنامج «تور»: كيف استهدفت «وكالة الأمن القومي» إخفاء الهويّة لمستخدمي الإنترنت».

Guardian,

http://www.theguardian.com/world/2013/oct/04/tor-attacks-nsa-users-online-anonymity

45. غلين غرينوالد وإدوارد سنودن (17 يوليو 2013). صحيفة الغارديان. مقال: «إدوار سنودن، مُطلق صافرة الإنذار، يجيب عن أسئلة القرّاء».

Guardian,

http://www.theguardian.com/world/2013/jun/17/edward-snowden-nsa-files-whistleblower

46. هناك نقاش عن أخلاقيّات ذلك الأمر في الموضوع التالي. سيرج إيغلمان وكورماك هيرلي وبول س. فان أورشوت (سبتمبر 2013)، ورقة بحث: «أسواق التوظيفات في «اليوم صفر»: الأخلاقيّات والإملاءات».

http://www.nspw.org/papers/2013/nspw2013-egelman.pdf

47. ستيفن فراي (5 ديسمبر 2013). مقال: «المجهولون المعروفون: تحليل تجريبي عن ثغرات الأمن غير المعلنة».

https://www.nsslabs.com/system/files/public-report/files/The%20Known%20Unknowns_1.pdf.

48. آندي غرينبرغ (21 مارس 2012). مجلة فوربس. مقال: «تعرّف إلى الـ«هاكرز» الذين يبيعون للجواسيس أدوات تستطيع اختراق كومبيوترك (ويحصلون على أموال بستة أصفار لقاء ذلك)».

http://www.forbes.com/sites/andygreenberg/2012/03/21/meet-the-hackers-who-sell-spiesthe-tools-to-crack-your-pc-and-get-paid-six-figure-fees

تنفق روسيا وكوريا الشمالية أموالًا طائلة للحصول على أدوات «اليوم صفر». صحيفة نيويورك تايمس. نيكول بيلروث وديفيد سانغر (13 يوليو 2013). مقال: «الـ«هاكرز» يبيعون نقاط الضعف في شيفرة الكومبيوتر والدول تشتريها».

http://www.nytimes.com/2013/07/14/world/europe/nations-buyingas-hackers-sell-computer-flaws.html.

مكتب وزارة الدفاع (4 فبراير 2014). تقرير: «التطوّرات الأمنية والعسكرية في كوريا الشمالية 2013».

http://www.defense.gov/pubs/North_Korea_Military_Power_Report_2013-2014.pdf

49. دانشو دانشيف (2 نوفمبر 2008). مقال: «السوق السوداء لثغرات «اليوم صفر» تنمو باطّراد».

http://www.zdnet.com/blog/security/black-market-for-zero-day-vulnerabilities-still-thriving/2108

50. هناك بحوث قيّمة في ذلك الصدد. إريك ريسكورولا (7 فبراير 2005). تقرير: «هل البحث عن ثغرات أمنيّة فكرة جيّدة؟».

http://www.rtfm.com/bugrate.pdf.

ســاندي كلارك (ديســمبر 2010). جامعة أوســتن، ولاية تكســاس. بحث: «الألفة تولّد الاحتقار: تأثير «شــهر العسل» ودور إرث التشفير في ثغرات «اليوم صفر»».
26th Annual Computer Security Applications Conference, Austin, Texas,
http://dl.acm.org/citation.cfm?id=1920299
آندي أوزمنت وســتيوارت شيشتر (11 مايو 2006). «مختبر لينكولن في معهد ماساشوستس للتقنية». بحث: «حليب أو نبيذ: هل يتحسّن أمن البرامج الرقمية مع الزمن؟».
MIT Lincoln Laboratory,
http://research.microsoft.com/pubs/79177/milkorwine.pdf

51. ويغدو الأمر أشــد ســوءاً مع «إنترنت الأشياء» والبرامج المتكاملة. بروس شناير (6 يونيو 2014). مجلة وايرد. مقال: «إنترنت الأشياء فاقدة للأمن بشكل واسع، وثغراتها غير قابلة للإغلاق».
Wired,
http://www.wired.com/2014/01/theres-no-good-way-to-patch-the-internet-of-things-and-thats-a-huge-problem

52. جيمــس بول وجوليان بورغر وغلين غرينوالد (5 ســبتمبر 2013). صحيفة **الغارديان**. مقال: «كشــف أخيراً: تآزر وكالات التجسّس الأميركيّة والبريطانيّة في هزيمة الخصوصيّة والأمن على الإنترنت».
Guardian,
http://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security

53. ظهرت النقاط الأربع في الوثيقة التالية. دانيال كاهيل (29 يوليو 2014). «خســائر الرقابة: تأثير «وكالة الأمن القومي» في الاقتصاد، حرية الإنترنت والفضاء السبراني».
http://www.newamerica.net/publications/policy/surveillance_costs_the_nsas_impact_on_the_economy_internet_freedom_cybersecurity

54. ميتشــل دانيــال (28 أبريل 2014). المدوّنــة الإلكترونيّة للبيت الأبيض. مقال: «ثغــرة «هارت بليد»: شرح عن سياق الكشف عن ثغرات سبرانيّة».
White House Blog,
http://www.whitehouse.gov/blog/2014/04/28/heartbleed-understanding-when-we-disclose-cyber-vulnerabilities.

55. رايــان ناريــان (14 ســبتمبر 2010). مجلة زد نِــت. مقال: «هجوم «ســتاكس نت» اســتنفد احتياطيّات لدى «مايكروسوفت» تكفي 4 أيام من ثغرات «اليوم- صفر»».
ZDNet,
http://www.zdnet.com/blog/security/stuxnet-attackers-used-4-windows-zero-day-exploits/7347

56. أندريا بيترسون (4 أكتوبر 2013). صحيفة **واشنطن بوست**. مقال: «لماذا نصبح كلّنا أقل أماناً عندما تمتنع «وكالة الأمن القومي» عن إصلاح ثغرات الأمن السبراني؟»
Washington Post,
http://www.washingtonpost.com/blogs/the-switch/wp/2013/10/04/why-everyone-is-left-lesssecure-when-the-nsa-doesnt-help-fix-security-flaws.

57. ديفيد ســانغر (12 أبريل 2014). صحيفة **نيويورك تايمس**. مقال: «وفق رســميّين: أوباما يسمح لـ «وكالة الأمن القومي» باستغلال بعض ثغرات الإنترنت».
http://www.nytimes.com/2014/04/13/us/politics/obama-lets-nsa-exploit-some-internet-flaws-officials-say.html.
كيم زيتر (15 أبريل 2014). مجلة وايرد. مقال: «أوباما يقول إن «وكالة الأمن القومي» ملزمة بالكشــف عن ثغرات كـ«هارت بليد»، إلا إذا كانت تستفيد منها».
Kim Zetter (15 Apr 2014),
«Obama: NSA must reveal bugs like Heartbleed, unless they help the NSA,»
Wired,

http://www.wired.com/2014/04/obama-zero-day.

58. جرت محاولات من ذلك القبيل. آندي أوزماند (يونيو 2005). جامعة كامبردج. بحث: «إمكانية إعادة اكتشاف ثغرة، والجدوى الاجتماعية من تصيّد الثغرات».

http://infosecon.net/workshop/pdf/10.pdf.

59. روبرت آكسلرود وورومان إلييف (28 يناير 2014). مقال: «توقيت الصراع السبراني».

http://www.pnas.org/content/early/2014/01/08/1322638111.full.pdf.

60. هناك مقال جميل يشرح بأسلوب غير تقني «الأبواب الخلفيّة». سردار يوغولالب (13 يونيو 2014). مجلة تيك ورلد. مقال: «الأبواب الخلفيّة الأشد ضخامة وجرأة وسوءاً في التاريخ».

Tech World,

http://www.techworld.com.au/slideshow/547475/pictures_biggest_baddest_boldest_software_backdoors_all_time

61. جيمس بول وجوليان بورغر وغلين غرينوالد (5 سبتمبر 2013). صحيفة الغارديان. مقال: «كشف أخيراً: تآزر وكالات التجسّس الأميركيّة والبريطانيّة في هزيمة الخصوصيّة والأمن على الإنترنت».

Guardian,

http://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security

صحيفة الغارديان، مقال (5 سبتمبر 2013). «مشروع «بول ران»: دليل تصنيفي إلى برنامج «وكالة الأمن القومي» في كسر التشفير».

62. «وكالة الأمن القومي» (2012). «مشروع تمكين سيغينت».

http://www.propublica.org/documents/item/784285-sigint-enabling-project.html.

63. لورنزو فرانشيسي- بيشياراي (11 سبتمبر 2013). موقع «ماشابل». مقال: «هل ضغطت «وكالة الأمن القومي» على «مايكروسوفت» للحصول على منفذ لشيفرة برمجيّاتها؟»

Mashable,

http://mashable.com/2013/09/11/fbi-microsoft-bitlocker-backdoor.

64. جيس إمسباك (16 أغسطس 2012). شبكة «آن بي سي نيوز». «الأبواب الخلفيّة التي تدسها الـ«إف بي آي» للرقابة، ربما تفتح أبواباً أمام الـ«هاكرز»».

NBC News,

http://www.nbcnews.com/id/48695618/ns/technology_and_science-security/t/fbi-surveillance-backdoor-might-open-door-hackers

بروس شناير (29 مايو 2013). مجلة فورين بوليسي. مقال: «الخطة الجديدة للتنصّت التي رسمتها الـ«إف بي آي»، تحمل أخباراً طيّبة للمجرمين».

Bruce Schneier (29 May 2013),

«The FBI's new wiretap plan is great news for criminals,» *Foreign Policy,*

http://www.foreignpolicy.com/articles /2013/05/29

65. سوزان لانداو (2011). كتاب: رقابة أم أمن؟ المخاطر المتأتيّة من التقنيات الجديدة في التنصّت.

http://mitpress.mit.edu/books/surveillance-or-security.

صحيفة نيويورك تايمس (21 سبتمبر 2013). مقال: «أغلقوا «الأبواب الخلفية» لـ«وكالة الأمن القومي»».

New York Times,

http://www.nytimes.com/2013/09/22/opinion/sunday/close-the-nsas-back-doors.html

66. فاسيلس بريفيلاكس ديوميدس سبينيلليس (29 يونيو 2007). مقال: «القضيّة الأثينيّة».

http://spectrum.ieee.org/telecom/security/the-athens-affair.

67. آلكسندر سمولتسزيك (5 أكتوبر 2006). صحيفة دير شبيغيل. مقال: «التجسّس على «لابيلا فيتا» [كناية عن إيطاليا]: الإصغاء بهدوء في إيطاليا».

Der Spiegel,

http://www.spiegel.de/international/spiegel/eavesdropping-on-la-bella-vita-listening-quietly-in-italy-a-440880.html.

جون لايدن (14 أبريل 2008). مقال: «برياتوني يكسر الصمت بخصوص أداة التجسّس على شركة «تيليكوم إيطاليا»».

http://www.theregister.co.uk/2008/04/14/telecom_italia_spying_probe_update

68. بروس شناير (23 يناير 2010). شبكة «سي آن آن». مقال: «الولايات المتحدة تمكّن صينيّين من اختراق «غوغل»».

CNN,

http://www.cnn.com/2010/OPINION/01/23/schneier.google.hacking/index.html

69. سوزان لانداو (23 مارس 2012). مقال: «الآلة الأبدية الضخمة والقنبلة الموقوتة».

http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2028152

70. البروفسور لورانس ليسيغ (20 أكتوبر 2014). مقابلة بواسطة «يوتيوب». «الفساد المؤسّساتي و«وكالة الأمن القومي»: لورانس ليسيغ يحاور إدوارد سنودن».

YouTube,

http://www.youtube.com/watch?v=DksIFG3Skb4

71. ريان ديفيرو، غلين غرينوالد ولورا بيوتراس (19 مايو 2014). قراصنة البيانات في الكاريبي: «وكالة الأمن القومي» تسجّل المكالمات الخلوية كافة في الـ«باهاماس».

Intercept,

https://firstlook.org/theintercept/article/2014/05/19/data-pirates-caribbean-nsa-recording-every-cell-phone-call-bahamas

72. وكالة الأمن القومي (2012). «مشروع تمكين سيغينت».

http://www.propublica.org/documents/item/784285-sigint-enabling-project.html.

73. كريغ تيمبرغ وآشكان سلطاني (14 ديسمبر 2013). صحيفة واشنطن بوست. «حطمت «وكالة الأمن القومي» نظام التشفير للاتصالات التليفونيّة العامة».

Washington Post,

http://www.washingtonpost.com/business/technology/by-cracking-cellphone-code-nsa-has-capacityfor-decoding-private-conversations/2013/12/13/e119b598-612f-11e3-bf45-61f69f54fc5f_story.html.

74. دان شومو ونيلز فيرغسون (21 أغسطس 2007). شركة «مايكروسوفت». مقال: «عن إحدى الاحتمالات بشأن وجود «باب خلفي» في نظام «نِست»».

http://rump2007.cr.yp.to/15-shumow.pdf.

دي. دبليو. (18 سبتمبر 2013). موقع «كريبتوغرافي ستاك إكستشينج». مقال: «شرح للجمهور عن ضعف شيفرة «ديوال-إي سي-بي آر إن»».

Cryptography Stack Exchange,

https://crypto.stackexchange.com/questions/10417/explaining-weakness-of-dual-ec-drbg-to-wider-audience

75. رايان غالاهار وغلين غرينوالد (12 مارس 2014). موقع «إنترسبت». «خطة «وكالة الأمن القومي» لنشر برمجيّات خبيثة في ملايين الحواسيب».

Intercept,

https://firstlook.org/theintercept/article/2014/03/12/nsa-plans-infect-millions-computers-malware.

76. غلين غرينوالد (14 يوليو2014). موقع «إنترسبت». مقال: «سرقة استطلاعات الرأي الشبكيّة والطرق الأخرى التي يستخدمها جواسيس بريطانيّون للسيطرة على الإنترنت».

Intercept,

https://firstlook.org/theintercept/2014/07/14/manipulating-online-polls-ways-british-spies-seek-control-internet.

77. بروس شناير (21 مايو 2014). موقع «شناير أون سكيوريتي». مقال: «وكالة الأمن القومي ليست سحراً».
Schneier on Security,
https://www.schneier.com/blog/archives/2014/05/the_nsa_is_not_.html
78. نيكولاس ويفر (13 مايو 2014). مجلة وايرد. مقال: «نظرة عن قرب لإحدى أقوى أدوات «وكالة الأمن القومي» لشن هجمات بواسطة الإنترنت».
Wired,
http://www.wired.com/2014/03/quantum.
Matt Brian (20 Jun 2014), «Hackers use Snowden leaks to reverse-engineer NSA surveillance devices,» *Engadget,*
http://www.engadget.com/2014/06/20/nsa-bugs-reverse-engineered.
79. بروس شناير (4 أكتوبر 2013). صحيفة الغارديان. مقال: «الجهوم على برنامج «تور»: كيف استهدفت «وكالة الأمن القومي» إخفاء الهويّة لمستخدمي الإنترنت».
Guardian,
http://www.theguardian.com/world/2013/oct/04/tor-attacks-nsa-users-online-anonymity
80. تعرّفت إلى برنامج «كوانتوم» منذ بداية تلك القصة. نيكولاس ويفر (13 مايو 2014). مجلة وايرد. مقال: «نظرة عن قرب لإحدى أقوى أدوات «وكالة الأمن القومي» لشن هجمات بواسطة الإنترنت».
Wired,
http://www.wired.com/2014/03/quantum
صحيفة دير شبيغيل (30 ديسمبر 2013). مقال افتتاحي: «وفق وثيقة لـ«وكالة الأمن القومي»: هكذا اخترقت حسابات سريّة على الإنترنت».
Der Spiegel,
http://www.spiegel.de/fotostrecke/nsa-dokumente-so-uebernimmt-der-geheimdienst-fremde-rechner-fotostrecke-105329.html.
صحيفة دير شبيغيل (30 ديسمبر 2013). مقال افتتاحي: «وفق وثيقة لـ«وكالة الأمن القومي»: حتى جهاز الاستخبارات السري كان عرضة لاختراق إلكتروني خارجي».
Der Spiegel,
http://www.spiegel.de/fotostrecke/nsa-dokumente-so-uebernimmt-der-geheimdienst-fremde-rechner-fotostrecke-105329.html.
81. نيكولاس ويفر وروبن سومر وفيرن باكسون (فبراير 2009). «منتدى عن الحوسبة الموزّعة وأمن الشبكات»، جامعة «سان دييغو» بكاليفورنيا. «تقصّي حزم الباكيت المزيّفة لـ«بروتوكول التحكّم بالبث» على الإنترنت».
Network and Distributed System Security Symposium (NDSS 2009), San Diego, California, http://www.icir.org/vern/papers/reset-injection.ndss09.pdf
82. مورغان ماركيز- بوار (15 أغسطس 2014). جامعة تورنتو، «مختبر المواطن»، «مركز مونك للدراسات الدوليّة». بحث: «شريط فيديو «قطّة شرودنغر» وموت النص الصريح على الإنترنت».
Citizen Lab, Munk School of Global Affairs, University of Toronto,
https://citizenlab.org/2014/08/cat-video-and-the-death-of-clear-text.
مورغان ماركيز- بوار (15 أغسطس 2014). موقع «إنترسبت». مقال: «سيخترق حاسوبك بمجرد مشاهدتك هذا الفيديو عن «قطة شرودنغر»».
Intercept,
https://firstlook.org/theintercept/2014/08/15/cat-video-hack.
كورا كوري ومورغان ماركيز- بوار (30 أكتوبر 2014). موقع «إنترسبت». تقرير: «كتب سريّة تظهر بيع برامج تجسّس رقمي للشرطة والمتسلّطين في العالم».
Intercept,
https://firstlook.org/theintercept/2014/10/30/hacking-team
83. موقع «إربوين». (27 مايو 2009). برنامج «إربوين 4.0».

Sourceforge,
http://airpwn.sourceforge.net/Airpwn.html.

84. توم سـيمونايت (19 سبتمبر 2012). مجلة معهد ماساشوسـتس للتقنية. مقال: «تقنيات «ستاكس نت» استنسخها مجرمو الكومبيوتر».
MIT Technology Review,
http://www.technologyreview.com/news/429173/stuxnet-tricks-copied-by-computer-criminals

85. آنـدي غرينـبرغ (2 سـبتمبر 2014). مجلة وايرد. مقـال: «أداة تقنيـة مخصّصة للبوليس، صـارت أداة بيد منحرفين للحصول على صور عارية من سحابة «آي كلاود» لشركة «آبل»».
Wired,
http://www.wired.com/2014/09/eppb-icloud.

86. موقع شركة «موبي ستيلث» (2014). مقال: «البرنامج الرقمي الأفضل لتتبّع الهواتف الخلوية».
http://www.mobistealth.com.

87. جاراد شرير (26 فبراير 2013). شركة «سيمانتك». مقال: «دبليو32.ستاكس نت».
http://www.symantec.com/security_response/writeup.jsp?docid=2010-071400-3123-99

88. ماثيو ي. شـفارتز (12 نوفمبر 2012). مجلة إنفورمايشـن ويك. مقال: «نيران صديقة من «ستاكس نت»: إصابة شركة «شيفرون»».
Information Week,
http://www.darkreading.com/attacks-and-breaches/cyber-weapon-friendly-fire-chevron-stuxnetfallout/d/d-id/1107339.

89. روبرت ماكميلان (14 سـبتمبر 2010). مجلة عالم الكومبيوتر. مقال: «شركة «سـيمنز»: فيروس «ستاكس نت» أصاب نظماً صناعيّة».
Computer World,
http://www.computerworld.com/s/article/9185419/Siemens_Stuxnet_worm_hit_industrial_systems

90. جيفري كار (29 سبتمبر 2010). مجلة فوربس. مقال: «هل أصاب فيروس «ستاكس نت» القمر الاصطناعي الهندي «إنسات- 4 بي؟»».
Forbes,
http://www.forbes.com/sites/firewall/2010/09/29/did-the-stuxnet-worm-kill-indias-insat-4b-satellite

91. جيمس بامفورد (13 أغسطس 2014). مجلة وايرد. مقال: «إدوارد سنودن: القصة غير المعلنة».
Wired,
http://www.wired.com/2014/08/edward-snowden.

92. مقال غير موقّع (يوليو 2012). «أضرار جانبيّة لتقنية «حَقِنْ نظام أسماء النطاق» تشمل حجب الإنترنت».
http://www.sigcomm.org/sites/default/files/ccr/papers/2012/July/2317307-2317311.pdf

93. أيـان بريمـر (18 نوفمبر 2013). مجلـة فورين آفيرز. مقـال: «الشرعيّة المفقودة: لماذا صار الحوكمة أشـد صعوبة مما مضى».
Foreign Affairs,
http://www.foreignaffairs.com/articles/140274/ian-bremmer/lost-legitimacy

94. فيفيـان والـت (30 يونيو 2013). مجلة تايم. مقـال: «غضب عارم يجتاح رسـميّين أوروبيّين إثر مزاعم عن تجسّس «وكالة الأمن القومي» على دبلوماسيّين أصدقاء لأميركا».
Time,
http://world.time.com/2013/06/30/european-officials-infuriated-by-alleged-nsa-spying-on-friendly-diplomats.

آن غيران (21 أكتوبر 2013). صحيفة واشنطن بوست. مقال: «تقرير عن تسجيل «وكالة الأمن القومي» الأميركيّة مكالمات تليفونيّة لفرنسيّين، يسبب صداعاً دبلوماسيّاً لأميركا».

Washington Post,
http://www.washingtonpost.com/world/national-security/report-that-nsa-collectedfrench-phone-records-causing-diplomatic-headache-for-us/2013/10/21/bfa74f22-3a76-11e3-a94f-b58017bfee6c_story.html

ماثيو كارنيتشنيغ (9 فبراير 2014). صحيفة وول ستريت جورنال. مقال: «فضيحة «وكالة الأمن القومي» ترهق العلاقات مع أوروبا».

Wall Street Journal,
http://online.wsj.com/news/articles/SB10001424052702303874504579372832399168684

95. ديفيد إي. سانغر (1 مايو 2014). صحيفة نيويورك تايمس. مقال: «الولايات المتحدة وألمانيا تفشلان في الاتفاق بشأن التجسّس».

New York Times,
http://www.nytimes.com/2014/05/02/world/europe/us-and-germany-fail-to-reach-a-deal-on-spying

مارك لاندر (2 آيار 2014). صحيفة نيويورك تايمس. مقال: «ميركل تشير إلى استمرار التوتر مع أميركا بشأن التجسّس».

New York Times,
http://www.nytimes.com/2014/05/03/world/europe/merkelsays-gaps-with-us-over-surveillance-remain.html.

96. خوان فوريرو (17 سبتمبر 2013). صحيفة واشنطن بوست. مقال: «فضيحة تجسّس «وكالة الأمن القومي» تفسد عشاء الرئيسة البرازيليّة في البيت الأبيض».

Washington Post,
http://www.washingtonpost.com/world/nsa-spying-scandal-spoils-dinner-at-the-white-house-for-brazils-president/2013/09/17/24f5acf6-1fc5-11e3-9ad0-96244100e647_story.html

الفصل 12: المبادئ

1. تتناول الكتب التالية تلك المواضيع بالنقاش. دانيال ج. سولوف (نوفمبر/ ديسمبر 2007). مقال: «ليس لديّ ما أخفيه، والمفاهيم المغلوطة الأخرى عن الخصوصيّة».

http://papers.ssrn.com/sol3/papers.cfm?abstract_id=998565

سوزان لانداو (2011). كتاب: **رقابة أم أمن؟ المخاطر المتأتية من التقنيات الجديدة في التنصّت.**

http://mitpress.mit.edu/books/surveillance-or-security.

2. تفسرّ سيكولوجيّة الأمن كثيراً من سلوكياتنا. بروس شناير (يونيو 2008)، نص: «سيكولوجيّة الأمن»، مداخلة في منتدى سيرج فوديناي «التقدّم في علم التشفير: أفريكريبت 2008»: المؤتمر الأول للتشفير في أفريقيا (الدار البيضاء- المغرب).

https://www.schneier.com/paper-psychology-of-security.pdf

دانيال غاردنر (2008)، كتاب: **علم الخوف: لماذا نخاف مما لا يجب خشيته، ونعرّض أنفسنا لمخاطر أكبر.**

The Science *of Fear: Why We Fear Things We Shouldn't—And Put Ourselves in Greater Danger, Penguin, http://books.google.com/books?id=bmyboRubog4C.*

3. بديهي القول إنّ التكاليف تصيب الناس بصورة متفاوتة. إذ يخشى الساسة من لومهم عند حصول هجمات

مستقبلًا، فيكون لديهم حافز لإشهار إجراءات الأمن الظاهرة. ويضحي المواطنون، خصوصاً أعضاء المجموعات السياسيّة والدينيّة المفتقدة للشعبيّة أهدافاً واضحة للرقابة؛ لكنهم يفتقدون ما يكفي من التماسك والقوة لمقاومتها. وتتسم البرامج الواسعة في الأمن بارتفاع كلفتها، ما يعود بالفائدة على المتعاقدين مع الحكومة والساسة المؤيّدين لهم.

4. في الورقة التالية، هناك محاولة لصنع نموذج عن ذلك استناداً إلى «نظرية اللعب». تيبريو دراغو (فبراير 2011). مجلة **أميركان بوليتيكال ساينس ريفيو**. ورقة بحث: «هل هناك مبادلة بين الأمن والخصوصيّة؟ الافتراضات القبليّة عند السلطة التنفيذيّة، حماية الخصوصيّة ودرء الإرهاب».
http://journals.cambridge.org/download.php?file=%2FPSR%2FS0003055410000614a.pdf&code=193cd836312527364579326df0a7aa58

5. سوزان لانداو (2011). كتاب: **رقابة أم أمن؟ المخاطر المتأتية من التقنيات الجديدة في التنصّت**.
http://mitpress.mit.edu/books/surveillance-or-security.

6. «مؤسّسة الحدود الإلكترونيّة» (28 نوفمبر 2012). تقرير: «كيف تحمي عدم انكشاف هويّتك على الإنترنت باستخدام برنامج «تور»».
https://www.eff.org/sites/default/files/filenode/Basic_Tor_Intro_Guide_FNL.pdf.

7. بالطبع، يحاول كثيرون الأمر عينه. روجر دينغلدين (30 يوليو 2014). المدوّنة الإلكترونيّة لمشروع «تور». مقال: «مستشارية «تور»: «التوصيل مبكراً» تأكيد لهجمة على الحراك الإلكتروني».
https://blog.torproject.org/blog/tor-security-advisory-relay-early-traffic-confirmation-attack

8. وكالة الأمن القومي (8 يناير 2007). مذكّرة «برنامج «تور» مثير للقرف».
http://cryptome.org/2013/10/nsa-tor-stinks.pdf.

9. كيفن بولسن (5 أغسطس 2014). مجلة وايرد. مقال: «زيارة موقع خطأ يكلّفك وصول الـ«إف بي آي» إلى كومبيوترك».
Wired,
http://www.wired.com/2014/08/operation_torpedo.

10. ليو كيليون (22 أغسطس 2014). هيئة الإذاعة البريطانيّة. «عملاء «وكالة الأمن القومي» و«القيادة الحكوميّة للاتّصالات» سرّبوا الأخطاء المكتشفة في برنامج «تور»، وفق مزاعم مطوّريه».
BBC News,
http://www.bbc.com/news/technology-28886462.

11. أنطوني زرشر (31 أكتوبر 2013). هيئة الإذاعة البريطانيّة. مقال: «من الإمبراطوريّة الرومانيّة إلى «وكالة الأمن القومي»: تاريخ التجسّس في العالم».
BBC News,
http://www.bbc.com/news/magazine-24749166

12. جون كاردويل (شتاء 1978). مجلة **دراسات الاستخبارات**. مقال: «قصة من التوراة عن التجسّس».
Studies in Intelligence,
http://southerncrossreview.org/44/cia-bible.htm

13. ثمة نقاش مهم وشائك يجب إثارته عن المخاطر النسبيّة للإرهاب، وقدرة الإرهاب على إحداث أضرار باستخدام التقنيّات التي باتت متاحة لهم؛ لكنه أمر يتجاوز حدود الكتاب. بروس شناير (14 مارس 2013). مجلة وايرد. مقال: «نماذجنا عن الأمن لن تنجح أبداً، مهما فعلنا».
Wired,
http://www.wired.com/2013/03/security-when-the-badguys-have-technology-too-how-do-we-survive

14. بالطبع، مسألة الثقة أقل عقلانيّة من ذلك. بروس شناير (2012). كتاب: **كَذَبَة ومتمرّدون: تفعيل الثقة التي يحتاجها المجتمع لينمو**. دار «ويلي» للنشر.
http://www.wiley.com/WileyCDA/WileyTitle/productCd-1118143302.html.

15. في المؤسّسات، هناك دوماً حاجة إلى فقاقيع معزولة من السريّة، كي يتمكن الناس من أداء أعمالهم في المؤسّسة بطريقة مناسبة، كالتصويت على مدّة ولاية لجنة ما أو المداولات بصدد قرار إشكالي. إذ يؤدّي جعل تلك الأشياء

إلى إنقاص استقلاليّة عملية اتّخاذ القرار. إذ ربما أضحى متّخذو القرار أكثر اهتماماً بالشكل الذي ستبدو عليه عملية اتّخاذ القرار، من اتّخاذهم قراراً صائباً.

16. أدريان لي وشـيلدون جاكوبسـن (مايو 2012). مقال: «التنبّه إلى شـكوك الركاب عن المخاطر بالنسبة لمسوح الأمن في المطارات».

http://pubsonline.informs.org/doi/abs/10.1287/trsc.1110.0384.

آليسـا فيكهام (7 مارس 2014). مقال: «وكالة أمن النقل» ترجئ برنامجاً للتدقيق في المعلومات الشـبكيّة عن المسافرين». مجلة لو 360.

http://www.law360.com/articles/516452/tsa-halts-program-to-screen-passengers-online-data

17. آمـبر توري (أبريـل 2008). «جامعـة براينت». مقـال: «التحليل التمايـزي الذي تجريه «مصلحـة المداخيل الداخلية» لتوقّع العائد المجزي لعملية تدقيق الدخل الفردي».

http://digitalcommons.bryant.edu/cgi/viewcontent.
cgi?article=1000&context=honors_mathematics

18. تبرز تلك الإشـكاليّة في المجتمع الشـفّاف الذي تخيّله المفكر ديفيد برين، بمعنى أن الشـفافيّة ليسـت مجانيّة. إذا طلـب ضابـط شرطة منك إبـراز هويّتك، لا يتحقّق التـوازن بأن تكون قادراً على طلب رؤيـة هويّته. ديفيد برين (1998). دار: «بازيك بوكس». كتاب: **المجتمع الشـفّاف: هل ترغمنا التكنولوجيا على الاختيار بين الخصوصيّة والحريّة؟**

http://www.davidbrin.com/transparentsociety1.html

19. صاغ «حزب قراصنة الكومبيوتر» في «أيسـلندا» (نعم، إنّه حـزب حقيقي)، الأمر ببراعة في 2014، وقال: «حق الأفـراد في الخصوصيّة يعني حماية الأضعف من تسـلط الأقوى، كما تعني الشـفافيّة انفتاح القوي على رقابة مـن لا قوّة بيده». بول فونتين (19 أغسـطس 2014). مجلة غرايبفاين. مقـال: «رئيس الوزراء يتعلّم معنى «الشفافيّة»».

http://grapevine.is/news/2014/08/19/prime-minister-learns-what-transparency-means

20. بالطبع، ثمة استثناءات لهذا القانون. هناك فائدة من وضع سوار تتبع إلكتروني على كواحل من أُدينوا بجرائم، حتى لو أدى الأمر إلى تقليل قوّة مراقبة المجرمين.

21. بيـتر واتـس (9 مايـو 2014). بحث: «مجتمع الأرض المحروقـة: دليل المفجّر الانتحـاري إلى الخصوصيّة على الإنترنت».

http://www.rifters.com/real/shorts/TheScorchedEarthSociety-transcript.pdf.

22. راي سانشـير (19 يوليو 2010). شبكة «إيه بي سي نيوز». مقال: «زيادة عدد الملاحقات بسبب أشرطة فيديو للشرطة».

http://abcnews.go.com/US/TheLaw/videotaping-cops-arrest/story?id=11179076.

23. تلك القرارات القانونيّة ليسـت دسـتوريّة. كاثرين مارشوسكي (25 مايو 2014). مقال: «محكمة قضت بحق رئيس «مشروع الدولة الحرّة» في تسجيل بوليس دائرة «ويير» أثناء توقّف حركة المرور».

http://www.unionleader.com/apps/pbcs.dll/article?AID=/20140525/NEWS07/140529379

24. ديفيد ليبيسـكا (27 ديسـمبر 2011). موقع «سـيتي لاب». مقال: «عندما تسيء الشرطة اسـتخدام كاميرات المراقبة».

CityLab,
http://www.citylab.com/politics/2011/12/surveillance-cameras-threat-police-privacy/806

25. سارة ليبي (18 أغسطس 2014). موقع «سيتي لاب». مقال: «إذا رأيت رجال الشرطة مرتدين كاميرات، فلا تظن أنك ستشاهدها».
CityLab,
http://www.citylab.com/crime/2014/08/even-when-police-do-wear-cameras-you-cant-count-on-ever-seeing-the-footage/378690

26. كريس ماتيشزيزيك (14 أغسطس 2014). موقع «سي نت». مقال: «في «فيرغسون» بولاية «ميسوري»، الاضطراب يختبر الحق القانوني في تصوير الشرطة».
http://www.cnet.com/news/ferguson-unrest-tests-legal-right-to-film-police

هيلل إيتالي (19 أغسطس 2014). وكالة أسوشيتدبرس. مقال: «اعتقالات «فيرغسون» تطال 10 صحافيّين على الأقل».
Associated Press,
http://abcnews.go.com/Entertainment/wireStory/ferguson-arrests-include-10-journalists-25044845

27. بيتر سواير (يونيو 2016). جامعة بيركلي. بحث: «التناقص المستمر في دورة حياة الأسرار ومستقبل استخبارات الإشارات».
http://www.law.berkeley.edu/plsc.htm

28. جاكوب آبلباوم (23 أكتوبر 2013). صحيفة دير شبيغيل. مقال: «برلين تشكو هل تجسّست أميركا على هاتف المستشارة ميركل؟».
Der Spiegel,
http://www.spiegel.de/international/world/merkel-calls-obama-over-suspicions-us-tappedher-mobile-phone-a-929642.html

أيان تراينور وفيليب أولترمان وبول لويس (23 أكتوبر 2013). صحيفة الغارديان. مقال: «أنغيلا ميركل تهاتف أوباما: هل تتجسّس على هاتفي الخلوي؟».
Guardian,
http://www.theguardian.com/world/2013/oct/23/us-monitored-angelamerkel-german.

29. هناك كتاب جيّد عن الجاسوس السوفياتي كيم فيلبي يتحدّث عن جو النوادي في وكالات التجسّس. بن ماكنتاير (2014). دار «كراون». كتاب: **جاسوس بين أصدقاء: كيم فيلبي والخيانة العظمى**.
http://books.google.com/books?id=wIzIAgAAQBAJ.

30. تشارلز ستروس (18 أغسطس 2013). مجلة فورين بوليسي. مقال: «سباي كيدز [إشارة إلى فيلم هوليوودي عن اختلاف جيل الكومبيوتر عن الكبار في مهنة التجسّس- المترجم]».
http://www.foreignpolicy.com/articles/2013/08/28/spy_kids_nsa_surveillance_next_generation.

31. «مكتب الإدارة والميزانية» (فبراير 2014). تقرير: «مراجعة عمليات الملاءمة والأمن».
http://www.fas.org/sgp/othergov/omb/suitsec-2014.pdf.

32. «مدرسة آنبرغ للاتصالات والصحافة». (22 أبريل 2013). تقرير: «هل انتهت الخصوصيّة؟ دلائل من «مدرسة آنبرغ للاتصالات والصحافة» تشير إلى أن أجيال الألفيّة الثالثة يتبنّون وقائع مختلفة على الإنترنت».
USC Annenberg News,
http://annenberg.usc.edu/News%20and%20Events/News/130422CDF_Millennials.aspx.

ماري مايدن (21 مايو 2013). «مركز مشروع «بيو» لبحوث الإنترنت». تقرير: «مراهقون، «سوشال ميديا» وخصوصيّة».
Pew Research Internet Project,
http://www.pewinternet.org/files/2013/05/PIP_TeensSocialMediaandPrivacy_PDF.pdf.

33. إنصافاً، لا نعرف إن كان ذلك يعبّر عن اختلاف أساسي بين الأجيال، أو أنه مجرد معطى إحصائي تأتّت «شريحة أعمار» لجيل ما زال شاباً، مع إمكان أن تتغيّر الصورة مع تقدّمه في العمر وتكاثر الأسرار المهمّة.

34. أفكر بالسريّة المؤسّساتيّة كأنها علاج كيمياوي للسرطان. يصح القول إن تلك الأدوية تقتل الإنسان ببطء، لكنها تقتل السرطان بسرعة كبيرة، فيكون الفارق نافعاً بالنتيجة. إذا توصّلنا إلى علاج يقتل السرطان ولا يؤثّر في الإنسان، حينها نتخلى بسرعة البرق عن العلاج الكيمياوي. عندما يظهر بديل للسريّة المؤسّساتيّة، يجب التخلّي عنها فوراً.

35. تشارلي روز (29 يوليو 2013). مقابلة: «الجنرال مايكل هايدن، المدير السابق لـ«سي آي إيه» و«وكالة الأمن القومي»، ومدير «شرتوف غروب»».

The Charlie Rose Show,
http://www.charlierose.com/watch/60247615

36. نسيم نيكولاس طالب وكونستانتين سانديس (1 أكتوبر 2013). مجلة **ريفيو أوف بيهيفيورال إيكونوميكس**. مقال: «التجريبيّة في اللعبة تحمي من ذيول الحوادث».
http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2298292.

37. كل مجتمع غير مبسّط ومتشدّد، يتعرّض لسقطات كارثيّة. تشارلز بيرو (1984). كتاب: **الحوادث الطبيعيّة: التعايش مع التكنولوجيّات العالية المخاطر**. «مطبعة جامعة برنستون».
https://encrypted.google.com/books?id=VC5hYoMw4N0C.

38. من الناحية النظريّة، يفترض أن يحمل هذا الضرب من التفكير شفاءً. كيفن غريفين (23 سبتمبر 2011)، صحيفة **هافنغتون بوست**. مقال: «الخطوة 9 من الشفاء البوذي للإدمان: حريّة عدم الكمال».
Huffington Post,
http://www.huffingtonpost.com/kevin-griffin/buddhist-addiction-recovery-step-9_b_958708.html

39. يعكوف ي. هايمس (أبريل 2009). **المجلة الدوليّة لتحليل المخاطر**. مقال: «عن تعريف النُظُم المرنة».
http://onlinelibrary.wiley.com/doi/10.1111/j.1539-6924.2009.01216.x/abstract

40. جيس روبنز (نوفمبر 2012). مقال: «هندسة المرونة: تعلّم احتضان الفشل».
Communications of the ACM 55,
http://queue.acm.org/detail.cfm?id=2371297.

41. جاءت بعض الأفكار من المصدر التالي. ووريجيا بومان وجان كامب (أبريل 2013). مجلة **إنوفيشن جورنال**. مقال: «حماية الإنترنت من الطغاة: حلول في التقنية والسياسة لتأمين الحريّات على الإنترنت».
Innovation Journal 18,
http://www.innovation.cc/scholarly-style/warigia_camp_bowman5edits18vi1a3.pdf.

42. جيمس بامفورد (2002). دار «آنكور» للنشر. كتاب: **جسد الأسرار: تشريح «وكالة الأمن القومي» الفائقة السريّة**.
http://www.randomhouse.com/features/bamford/author.html.

43. جاك غولد سميث (14 أبريل 2014). موقع «لو فير». مقال: «المفارقة السبرانيّة: كل سلاح هجومي هو (احتمالاً) جزء من نظامنا الدفاعي، والعكس بالعكس».
Lawfare,
http://www.lawfareblog.com/2014/04/cyber-paradox-every-offensive-weaponis-a-potential-chink-in-our-defense-and-vice-versa

44. ستيفاني بيل وسوغهويان (15 مايو 2014). مجلة **هارفرد جورنال أوف لو أند تكنولوجي**. بحث: «لم تعد «ستنغراي» سراً: الاحتكار الحكومي المتلاشي للرقابة على الخلوي وتأثيره في الأمن القومي وخصوصيّة المستهلك».
Harvard Journal of Law and Technology (forthcoming),
http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2437678

45. كيم زيتر (3 سبتمبر 2014). مجلة وايرد. مقال: «صنع «جدار نار» رقمي للهواتف يستطيع التعرّف إلى أبراج الخلوي الزائفة التي تعترض مكالماتك الهاتفيّة».
Wired,
http://www.wired.com/2014/09/cryptophone-firewall-identifies-rogue-cell-towers
آشكان سلطاني وكريغ تيمبرغ (17 سبتمبر 2014). صحيفة **واشنطن بوست**. مقال: «شركات التكنولوجيا ترفع الستار عن جهود الرقابة [الحكوميّة] في واشنطن».

Washington Post,
http://www.washingtonpost.com/world/nationalsecurity/researchers-try-to-pull-back-curtain-on-surveillance-efforts-in-washington/2014/09/17/f8c1f590-3e81-11e4-b03f-de718edeb92f_story.html

الفصل 13: حلول للحكومة

1. ريتشارد كلارك وآخرون (12 ديسمبر 2013)، «الحريّة والأمن في عالم متغيّر: تقرير وتوصيات «لجنة الرئاسة للمراجعة بشأن الاستخبارات وتقنيات الاتصالات»»، المكتب التنفيذي للرئيس الأميركي.
http://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf.
2. «مؤسّسة الحدود الإلكترونيّة» (مايو 2014) تقرير: «ضروري ومناسب: مبادئ دوليّة لتطبيق حقوق الإنسان على رقابة الاتصالات: عرض خلفيّة الموضوع والتحليل القانوني المساند».
https://en.necessaryandproportionate.org.
3. «مؤسّسة الحدود الإلكترونيّة» (5 يناير 2014) تقرير: «13 مبدأ دولياً لتطبيق حقوق الإنسان على رقابة الاتصالات».
https://necessaryandproportionate.org/files/2014/01/05/13p-onepagerfinal.pdf.
4. في مثل واحد على ذلك، قال جيمس كلابر، رئيس الاستخبارات القوميّة، إنّ «الكشف عن معلومات حول الطُرُق المحدّدة التي تستعملها الحكومة لجمع بيانات الاتّصالات، بإمكانه بوضوح أن يعطي أعداءنا ما يشبه «كتاب قواعد اللعب» لتجنّب اكتشافهم [من قِبَل الحكومة]». صحيفة نيويورك دايلي نيوز نقلاً عن وكالة أسوشيتدبرس في (9 يونيو 2013)، مقال: «دفاع رئيس الاستخبارات جيمس كلابر عن برنامج التجسّس على الإنترنت».
New York Daily News,
http://www.nydailynews.com/news/politics/intelligence-chief-james-clapper-defends-internet-spying-program-article-1.1367423.
5. في العام 2014، علمنا أن إسرائيل تنصّتت على الاتصالات الدبلوماسيّة بين وزير الخارجية جون كيري ودول مختلفة في الشرق الأوسط. صحيفة دير شبيغيل (3 أغسطس 2014). مقال افتتاحي: «تنصّت: إسرائيل تسترق السمع إلى محادثات كيري في الشرق الأوسط».
Der Spiegel,
http://www.spiegel.de/international/world/israel-intelligence-eavesdropped-on-phone-calls-by-john-kerry-a-984246.html
6. كونور فريدرسدورف (18 مارس 2014). مجلة آتلانتيك. مقال: «لماذا لا يوصف التعديل الرابع في الدستور بأنه سري؟».
Atlantic,
http://www.theatlantic.com/politics/archive/2014/03/why-isnt-the-fourth-amendment-classified-as-top-secret/284439
7. لنتذكّر أيضاً أنّ معظم ذلك تأتّى كرد فعل على إساءة الشرطة استعمال السلطة. ليس الأمر أنّ الشرطة أقل ميلاً لإساءة استخدام السلطة، بل إننا امتلكنا من الوقت ما كان كافياً لتطوير قوانين للسيطرة عليه.
8. بروس شناير (31 يوليو 2012). شبكة «سي آن آن». مقال: «استنتاج دروس مغلوطة من أحداث مخيفة».
CNN,
http://www.cnn.com/2012/07/31/opinion/schneier-aurora-aftermath/index.html
9. يطلق تقنيّو الأمن المعلوماتي على النُظُم الرقميّة غير الشفافة تسمية «الأمن بالتعمية». إذ يكون التصميم الجيّد للنُظُم إلى عكس ذلك، بمعنى أنها تكون فعّالة حتى لو علم الجميع بتفاصيلها كافة. بروس شناير (15 مايو 2002). كتاب كريبتو غرام: **السريّة، الأمن والتعمية**.
Crypto-Gram,

https://www.schneier.com/crypto-gram-0205.html#1.

10. مايكل سيلغليد (سبتمبر 2009). مجلة **منظمة الصحة العالمية**. تقرير: «سيطرة البحوث المزدوجة الاستخدام: إشكاليّة أخلاقيّة».

Bulletin of the World Health Organization 87,
http://www.who.int/bulletin/volumes/87/9/08-051383/en

كارل زيمر (5 مارس 2012). صحيفة **نيويورك تايمس**. مقال: «الهواة مصدر خوف جديد في صنع فيروسات متحوّلة».

New York Times,
http://www.nytimes.com/2012/03/06/health/amateur-biologists-are-new-fear-in-makinga-mutant-flu-virus.html.

مايكل سبكتر (12 مارس 2012). صحيفة **نيويوركر**. مقال: «الفيروس الأشد فتكاً».

New Yorker,
http://www.newyorker.com/magazine/2012/03/12/the-deadliest-virus

11. بيث كاسبر (أغسطس 2001). «مركز الاستراتيجيّة والتكنولوجيا» في «كلية الحرب الجويّة». ورقة بحث: «نهاية السريّة؟ التنافس العسكري في عصر الشفافية».

Strategy and Technology, Air War College, Air University, Maxwell Air Force Base, Alabama,
http://www.fas.org/sgp/eprint/kaspar.pdf.

12. «وكالة الأمن القومي» (31 أكتوبر 2013). تقرير: «نشاطات «وكالة الأمن القومي»: التركيز على الأهداف المنتقاة من [أفراد] الاستخبارات الأجنبيّة».

http://www.nsa.gov/public_info/press_room/2013/NSA_Activities_Valid_FI_Targets.pdf

13. في أحد تلك الآراء، لاحظ القاضي بايتس «أنّ «وكالة الأمن القومي» تجاوزت باستمرار المدى المخوّل لها في المصادرة». سبنسر إكرمان (19 نوفمبر 2013). صحيفة **الغارديان**. مقال: «الكشف للمرّة الأولى عن القرار القضائي من محكمة «فيسا» الذي أتاح لـ«وكالة الأمن القومي» ممارسة الرقابة».

Guardian,
http://www.theguardian.com/world/2013/nov/19/court-order-that-allowed-nsa-surveillance-is-revealed-for-first-time

يوشاي بنكلر (16 أكتوبر 2013). صحيفة **الغارديان**. مقال: «كيف تفسد الـ«إف بي آي» و«وكالة الأمن القومي» إشرافاً [حكوميّاً] ضعيفاً».

Yochai Benkler (16 Oct 2013), «How the NSA and FBI foil weak oversight,» *Guardian*,
http://www.theguardian.com/commentisfree/2013/oct/16/nsa-fbi-endrun-weak-oversight

مارسي ويلر (22 أغسطس 2014). مجلة **ويك**. مقال: «لهذه الأسباب، لا تستطيع الثقة بـ«وكالة الأمن القومي»، أبداً».

Week,
http://theweek.com/article/index/266785/this-is-why-you-canttrust-the-nsa-ever

14. بيتر ولستن (10 أغسطس 2013). صحيفة **واشنطن بوست**. مقال: «محامون يقولون إن عوائق انتصبت في وجه الإشراف على برنامج «وكالة الأمن القومي» في رقابة الهواتف».

Washington Post,
http://www.washingtonpost.com/politics/2013/08/10/bee87394-004d-11e3-9a3e-916de805f65d_story.html.

15. غلين غرينوالد (4 إغسطس 2013). صحيفة **الغارديان**. مقال: «أعضاء في الكونغرس يمنعون من معلومات أساسيّة عن «وكالة الأمن القومي»».

Guardian,

http://www.theguardian.com/commentisfree/2013/aug/04/congress-nsa-denied-access

16. إلزا تشـانغ (11 يونيو 2013). موقع «أولثنغز كونسـدرد». مقال: «ما الذي يعرفه الكونغرس حقاً عن ترصّد «وكالة الأمن القومي؟».

All Things Considered, NPR,
http://www.npr.org/blogs/itsallpolitics/2013/06/11/190742087/what-did-congress-really-know-about-nsatracking.

17. رون وايدن (29 يناير 2014). «خطاب وايدن أثناء جلسة استماع مفتوحة في مجلس الشيوخ».
http://www.wyden.senate.gov/news/press-releases/wyden-statement-at-senate-intelligence-committees-open-hearing

18. ديانا فاينشـتاين (28 أكتوبر 2013). تقرير: «خطاب ديانا فاينشـتاين بشـأن جمع الاستخبارات بيانات عن قادة أجانب».
http://www.feinstein.senate.gov/public/index.cfm/2013/10/feinstein-statement-on-intelligence-collection-of-foreign-leaders.

19. آلان غرايسون (25 أكتوبر 2013). صحيفة الغارديان. مقال: «إشراف الكونغرس على «وكالة الأمن القومي» هو نكتة. أنا أعرف ذلك، فأنا في الكونغرس».

Guardian,
http://www.theguardian.com/commentisfree/2013/oct/25/nsa-no-congress-oversight

20. بروس شـناير (16 يناير 2014). مدوّنة إلكترونيّة. مقال: «اليوم، قدّمت تلخيصاً للكونغرس عن «وكالة الأمن القومي»».

21. بيتر ولستن (10 أغسطس 2013). صحيفة واشنطن بوست. مقال: «محامون يقولون إن عوائق انتصبت في وجه الإشراف على برنامج «وكالة الأمن القومي» في رقابة الهواتف».

Washington Post,
http://www.washingtonpost.com/politics/2013/08/10/bee87394-004d-11e3-9a3e-916de805f65d_story.html.

22. جون نابير تاي (18 يوليو 2014). صحيفة واشنطن بوست. مقال: «شرح عن الأمر التنفيذي رقم 12333: قانون ريغان الذي أطلق يد «وكالة الأمن القومي» في التجسّس على الأميركيّين».
http://www.washingtonpost.com/opinions/meet-executive-order-12333-the-reagan-rule-that-lets-the-nsa-spy-on-americans/2014/07/18/93d2ac22-0b93-11e4-b8e5-d0de80767fc2_story.html

تشـارلي سـافاج وآليشـيا بارلبينو (13 أغسـطس 2014). صحيفة نيويـورك تايمس. مقـال: «مجموعتان متباينتان من القوانين للرقابة، إحداها لأميركا والثانية للأراضي الأجنبيّة».

New York Times,
http://www.nytimes.com/interactive/2014/08/13/us/two-sets-of-rules-for-surveillance.html.

آلين ناكاشيما وآشكان سلطاني (23 يوليو 2014). صحيفة واشنطن بوست. مقال: «الهدف التالي لمؤسّسة تدافع عن الخصوصيّة: الملمح الأضخم والأقل ظهوراً في رقابة «وكالة الأمن القومي»».

Washington Post,
http://www.washingtonpost.com/blogs/the-switch/wp/2014/07/23/privacywatchdogs-next-target-the-least-known-but-biggest-aspect-of-nsa-surveillance

تشارلي سـافاج (13 أغسطس 2014). صحيفة نيويورك تايمس. مقال: «وفق مساعد سابق: قانون للرقابة من زمن ريغان يتعدّى على الحقوق».

New York Times,

http://www.nytimes.com/2014/08/14/us/politics/reagan-era-order-on-surveillance-violates-rights-says-departing-aide.html.

23. آليكس آبدو (29 سبتمبر 2014). «وثائق جديدة تلقي الضوء على أقوى أدوات «وكالة الأمن القومي»».
Free Future,
https://www.aclu.org/blog/national-security/new-documents-shed-light-one-nsas-most-powerful-tools

24. مارسي ويلر (7 ديسمبر 2007). موقع «إيمبتي ويل». مقال: «البيت الأبيض يضبط متلبساً بتهمة الادعاء بعدم وجود قانون يضبطه».
Empty Wheel,
https://www.emptywheel.net/2007/12/07/whitehouse-rips-the-white-house

25. جوستين إليوت (17 يونيو 2013). موقع «بروبابليكا». مقال: «أتذكُر أيام انحصر النقاش عن «قانون باتريوت» بسجلات المكتبات؟»
Pro Publica,
http://www.propublica.org/article/remember-when-the-patriot-act-debate-was-about-libraryrecords

26. مايك مازنيك (17 سبتمبر 2013). موقع «تيك درت». مقال: «المحاكم تكشف «تفسيراً سريّاً» لـ«قانون باتريوت»، يتيح لـ«وكالة الأمن القومي» جمع بيانات الهواتف كلها».
Tech Dirt,
https://www.techdirt.com/articles/20130917/13395324556/court-revealssecret-interpretation-patriot-act-allowing-nsa-to-collect-all-phone-call-data.shtml

27. أندريا بيترسون (11 أكتوبر 2013). صحيفة **واشنطن بوست**. مقال: «مؤلّف «قانون باتريوت»: هناك فشل في الإشراف».
Washington Post,
http://www.washingtonpost.com/blogs/the-switch/wp/2013/10/11/patriot-act-author-therehas-been-a-failure-of-oversight.

28. جنيفر فالنتيو- ديفريز وسيوبهان غورمان (8 يوليو 2013). صحيفة **وول ستريت جورنال**. مقال: «إعادة تعريف محكمة سريّة لكلمة «دلالة» أعطت «وكالة الأمن القومي» سلطات واسعة في جمع البيانات».
Wall Street Journal,
http://online.wsj.com/news/articles/SB10001424127887323873904578571893758853344

29. مجلس الشيوخ الأميركي (26 أبريل 1976). وثيقة حكوميّة: «التقرير النهائي للجنة المنتدبة لدراسة عمليات الحكومة المتّصلة بنشاطات الاستخبارات. تأثير رقابة «وكالة الأمن القومي» في الأميركيّين».
http://www.aarclibrary.org/publib/church/reports/book3/pdf/ChurchB3_10_NSA.pdf

30. كاسبر باودن (23 أغسطس 2012). تقرير: «إقرار إلى «اللجنة المشتركة» بصدد مسودة «مشروع قانون بيانات الاتصالات»».
http://www.academia.edu/6002584/Submission_to_the_Joint_Committee_on_the_draft_Communications_Data_Bill

31. أثناء منازعة قانونيّة حديثة، وصفه قاضٍ بأنه «قانون صعب، بل لا نفاذ إلى مراميه»، وسمّاه مدّعي عام الحكومة نفسها بأنه «تشريع مملوء بالالتفافات». أوين بوكوت (18 يوليو 2014). صحيفة **الغارديان**. مقال: «الاستخبارات تصنع قواعد بيانات ضخمة من البريد الإلكتروني الذي تعترضه على الإنترنت».
Guardian,
http://www.theguardian.com/uk-news/2014/jul/18/intelligence-services-email-database-internet-tribunal.

32. تنطبق قوانين «الاتحاد الأوروبي» على المملكة المتحدة، وتعتدي الرقابة العامة تحت مظلّة «قانون تنظيم سلطات التحقيق»، على «الميثاق الأوروبي لحقوق الإنسان». نيك هوبكنز (28 يناير 2014). صحيفة **الغارديان**. مقال:

«المظلة الواسعة للرقابة العامة لـ«القيادة الحكوميّة للاتّصالات»، هي غير شرعيّة وفق محامٍ رفيع المستوى».
Guardian,
http://www.theguardian.com/uk-news/2014/jan/28/gchqmass-surveillance-spying-law-lawyer.

33. قـال الرئيـس أوباما إنّ برامج «وكالـة الأمن القومي» تجري «في ظل إشراف دقيق مـن الأذرع الثلاث للحكم». باراك أوباما (7 يونيو 2013)، صحيفة وول سـتريت جورنال، «مقتطفات من ملاحظات أوباما عن الجدال بشأن وكالة الأمن القومي».
Wall Street Journal,
http://blogs.wsj.com/washwire/2013/06/07/transcript-whatobama-said-on-nsa-controversy

34. «مركز معلومات الخصوصيّة الإلكترونيّة» (2014). تقرير: «قرارات المحاكم بشأن قانون مراقبة الاستخبارات الأجنبيّة: 1979-2014».
https://epic.org/privacy/wiretap/stats/fisa_stats.html

35. أثـار «الاتحـاد الأميركي للحريّات المدنيّة» نقاشـاً واسـعاً عن ضرورة الإصـلاح وأسـبابها. «الاتحاد الأميركي للحريّات المدنيّة» (2014). نداء: «أصلحوا البند 215 من «قانون باتريوت»».
https://www.aclu.org/free-speech-national-security-technology-and-liberty/reform-patriot-act-section-215

36. ناقـش «الاتحـاد الأميركي للحريّات المدنيّة» أيضـاً، الحاجة إلى إحداث إصلاح يتناول ذلـك الأمر. جميل جعفر (19 مـارس 2014). «إقـرار من جميل جعفر، نائـب المدير القانوني في «الاتحاد الأميركـي للحريّات المدنيّة»، عن جلسـة الاسـتماع العام لـ«هيئة الإشراف على الخصوصيّة والحريّات المدنيّة»، حول البند 702 من «قانون تعديلات عمل محكمة فيسا»».
http://www.pclob.gov/Library/Meetings-Events/2014-March-19-Public-Hearing/Testimony_Jaffer.pdf

37. جـرى حـوار متبـادل في «لجنـة الاسـتخبارات» في مجلس الشـيوخ، بـين السـيناتور رون وايـدن (عن ولاية «أوريغون»)، ومدير «وكالة الأمن القومي» حينها، آلكسـندر كيث. ووجّه وايدن إلى آلكسـندر سؤالاً عن تجميع الوكالة بشـكل واسـع لـ«البيانات المكانيّة» من هواتف الأميركيّين. وردّ آلكسـندر بأن الوكالة لم تجمعها تحت السلطة المناطة بها بموجب البند 215 من «قانون باتريوت». عندها، سأل وايدن من آلكسندر إيضاح إذا كانت الوكالة جمعت تلك البيانات بموجب تخويل قانوني آخر. ورفض آلكسـندر الإجابة. روبن غرين (27 سـبتمبر 2013). صحيفة واشـنطن مارك آب. مقال: «رسـمياً: تريـد «وكالة الأمن القومي» اغـتراف بيانات هواتف الأميركيّين كافة».
Washington Markup,
https://www.aclu.org/blog/national-security/its-official-nsa-wants-suck-all-americans-phonerecord

38. مارسي ويلر (14 أغسـطس 2014). موقع «إيميتي ويل». مقـال: «معظم الأوامر المتعلّقة بالبند 215، تتناول شركات إنترنت رفضت رسائل طلب كشف المعلومات من «وكالة الأمن القومي»».
Empty Wheel,
http://www.emptywheel.net/2014/08/14/the-bulk-of-215-orders-come-from-internet-companies-that-refuse-nsls

39. مارسي ويلر (23 يونيو 2014). مقال: «نظريّة الذراع الوحيد في الإشراف».
http://www.cato-unbound.org/2014/06/23/marcy-wheeler/single-branch-theory-oversight

40. ريتشارد كلارك وآخرون (12 ديسمبر 2013)، «الحريّة والأمن في عالم متغيّر: تقرير وتوصيات «لجنة الرئاسة للمراجعة بشأن الاستخبارات وتقنيات الاتصالات»»، المكتب التنفيذي للرئيس الأميركي.
http://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf.

41. باراك أوباما (17 يناير 2014). المكتب التنفيذي للرئاسة. تقرير: «ملاحظات من الرئيس عن لجنة مراجعة الاستخبارات».

US Executive Office of the President,
http://www.whitehouse.gov/the-press-office/2014/01/17/remarks-president-review-signalsintelligence

42. غاريت هاتش (27 أغسطس 2012). «خدمة بحوث الكونغرس». تقرير: «هيئة الإشراف بصدد الخصوصيّة والحريّات المدنيّة الوضع الجديد المستقل للوكالة».

Congressional Research Service,
http://www.fas.org/sgp/crs/misc/RL34385.pdf.

43. «الاتحاد الأميركي للحريّات المدنيّة» (2 يوليو 2014). تقرير: «هيئة إشراف حكومي تشير إلى غياب السند القانوني لكثير مما يتصل ببرنامج للرقابة في «وكالة الأمن القومي»».

https://www.aclu.org/national-security/government-privacy-watchdogsigns-much-nsa-warrantless-wiretapping-program

44. «هيئة الإشراف بصدد الخصوصيّة والحريّات المدنيّة» (2 يوليو 2014). وثيقة: «تقرير عن برنامج الرقابة الممارس بموجب البند 702 من «قانون مراقبة الاستخبارات الأجنبيّة»».

http://www.pclob.gov/All%20Documents/Report%20on%20the%20Section%20702%20Program/PCLOB-Section-702-Report.pdf

45. فريدريك أ. و. شفارتز جونيور (12 مارس 2014). صحيفة نايشن. مقال: «لماذا نحتاج إلى «شيرش كوميتي» لإصلاح نظامنا الاستخباراتي الفاشل».

Nation,
http://www.thenation.com/article/178813/why-we-need-new-church-committee-fixour-broken-intelligence-system

46. هناك مثلٌ عن ذلك في الموضوع التالي. غريغوري كونتي وليزا شاي وودرو هارتزوغ (صيف 2014). مقال: «تفكيك العلاقة بين الخصوصيّة والأمن».

http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=6824305.

47. جميل جعفر (19 مارس 2014). «إقرار من جميل جعفر، نائب المدير القانوني في «الاتحاد الأميركي للحريّات المدنيّة»، عن جلسة الاستماع العام لـ«هيئة الإشراف على الخصوصيّة والحريّات المدنيّة»، حول البند 702 من «قانون تعديلات عمل محكمة فيسا»».

http://www.pclob.gov/Library/Meetings-Events/2014-March-19-Public-Hearing/Testimony_Jaffer.pdf

48. مؤسّسة «برايفسي إس أو إس» (10 ديسمبر 2013). تقرير: «لا أدلة، لا قلق: عن استعمال مذكّرات الجلب السريّة».

http://www.privacysos.org/node/1263

49. آندرو نولان وريتشارد م. تومبسون الثاني وفيفيان س. شو (25 أكتوبر 2013). «خدمة بحوث الكونغرس». تقرير: «تعريف محامٍ عن العموم بالمحاكم المختصة بـ«قانون مراقبة الاستخبارات الأجنبيّة»: انتقاء القضايا القانونيّة».

http://fas.org/sgp/crs/intel/advocate.pdf.

كونفغتون وبرلينغ (مايو 2014). موقع «إنسايد برايفسي». مقال: «عن دستوريّة وجود محامٍ عن العموم لشؤون الخصوصيّة».

http://www.insideprivacy.com/files/2014/07/The-Constitutionality-of-a-Public-Advocate-for-Pri.pdf

50. جويل رايدنبرغ (2 نوفمبر 2013). ورقة (تحت الطبع): «حال بيانات الرقابة في أوروبا وأميركا».
http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2349269.

51. إدوارد سنودن (7 مارس 2014). «بيان إلى البرلمان الأوروبي».
http://www.europarl.europa.eu/document/activities/cont/201403/20140307ATT80674/20140307ATT80674EN.pdf

52. ميرك بوب (16 نوفمبر 2005). تقرير: «الإشراف الداخلي والخارجي على الشرطة في الولايات المتحدة».
http://www.parc.info/client_files/altus/10-19%20altus%20conf%20paper.pdf.

53. مايـكل ب. فاينبـك (3 يونيو 2010). مقـال: «المراقبة على المراقِبين: دروس للقـوى الفيدرالية لإنفاذ القانون، من المدن الأميركيّة».
http://www.wmitchell.edu/lawreview/documents/12.weinbeck.pdf

إدواردو ل. كالديـرون ومـاريـا هرنانديز- فيغورا (ينايـر 2013). جامعة كاليفورنيـا. مقال: «دور جمعيات المواطنين في الإشراف على قوى إنفاذ القانون».
http://cpp.fullerton.edu/cpp_policeoversight_report.pdf.

54. ديفيـد بـوزن (20 ديسـمبر 2013). مجلة هارفرد لو ريفيو. مقـال: «وحش ليفياثان المُسرِّب: كيف تدين الحكومة وتشجّع الكشف غير المشروع عن الوثائق».
Harvard Law Review 127,
http://harvardlawreview.org/2013/12/the-leaky-leviathan-why-the-government-condemns-and-condones-unlawful-disclosures-of-information.

راهول ساغار (20 ديسمبر 2013). مجلة هارفرد لو ريفيو. مقال: «صرير ليفياثان: تعليق على فكرة ديفيد بوزن عن وحش ليفياثان المُسرّب».
Harvard Law Review Forum 127,
http://cdn.harvardlawreview.org/wp-content/uploads/pdfs/forvol127_sagar.pdf.

55. يعـرض المقالان التاليان ذلك الموضوع. دانا بويد (19 يوليو 2013). موقع «آبوفينا». مقال: «إطلاق صافرات الإنذار بوصفه شكلًا جديداً للعصيان المدني: عن أهميّة سنودن».
apophenia,
http://www.zephoria.org/thoughts/archives/2013/07/19/edwardsnowden-whistleblower.html

ويليام ي. شـويارمان (سـبتمبر 2014). موقع «الفلسـفة والنقد الاجتماعي». مقال: «إطـلاق صافرة الإنذار بوصفه تمرّداً مدنيّاً: حال إدوارد سنودن».
Philosophy and Social Criticism 40,
http://psc.sagepub.com/content/40/7/609.abstract

56. ج. آليكس سنها (28 يوليو 2014). مؤسّسة «هيومن رايتس ووتش». مقال: «لديهم حريّة أن يراقبوا الجميع».
Human Rights Watch,
http://www.hrw.org/reports/2014/07/28/libertymonitor-all.

57. راهول ساغار (2013). «مطبعة جامعة برنستون». كتاب: **أسرار وتسريبات: الإشكاليّة في سريّة الدولة**.
http://press.princeton.edu/titles/10151.html

58. ماري- روز بابندريا (مارس 2014). مجلة بوسـطن يونيفرسـتي لو ريفيو. مقـال: «مسَرِّب خائن مُطلِق صافرة إنذار جاسوس: تسريبات «وكالة الأمن القومي» والتعديل الأول للدستور الأميركي».
http://www.bu.edu/bulawreview/files/2014/05/PAPANDREA.pdf

59. بروس شـناير (6 يونيو 2013). مجلة آتلانتيك. مقال: «ما لا نعرفه عن التجسّـس على المواطنين: إنهم أشـد ذعراً مما نعرف».
Atlantic,
http://www.theatlantic.com/politics/archive/2013/06/what-we-dont-know-about-spying-on-citizensscarier-than-what-we-know/276607

60. قدّم يوشاي بنكلر مؤشّرات تستطيع المحاكم الاستناد إليها في تقرير ذلك. يوشاي بنكلر (يوليو 2014). مجلة هارفرد ريفيو أوف لو أند بوليسي. بحث: «دفاع من وجهة الموثوقيّة الشعبيّة عن مسّربي وثائق «وكالة الأمن القومي» ومُطلقي صافرات الإنذار بشأنها».
Harvard Review of Law and Policy 8,
http://benkler.org/Benkler_Whistleblowerdefense_Prepub.pdf

61. يتبنّى يوشاي بنكلر فكرة أن الشيء الأشد ذكاءً الذي يجب على الولايات المتحدة فعله، هو إعطاء إدوارد سنودن حصانة قانونيّة، والسماح له بالعودة إلى الولايات المتحدة. يوشاي بنكلر (8 سبتمبر 2014). مجلة آتلانتيك. مقال: «أتريدون إصلاح «وكالة الأمن القومي»؟ إذاً، أعطوا إدوارد سنودن حصانة قانونيّة».

62. وزارة العمل (2014). يملك غلين راينولدز أفكاراً عن تعظيم الفائدة من إطلاق صافرة الإنذار إلى الحدّ الأقصى، مع تخفيض الأذى إلى الحدّ الأدنى. غلين راينولدز (15 سبتمبر 2014). شبكة بحوث العلوم الاجتماعيّة. مقال: «لا تخشى مُطلِق صافرة الإنذار: أفكار عن البيروقراطيّة والإطلاق الأخلاقي لصافرات الإنذار».
Social Sciences Research Network,
http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2496400

63. آكسل آرنباك (30 سبتمبر 2013). «مجلس الخصوصيّة والرقابة- لوزان، سويسرا». مقال: «السؤال الذي لا يطرحه المحامون: هل يستطيع القانون تأييد رقابة انتقاليّة شاملة؟».

Congress on Privacy and
Surveillance, Lausanne, Switzerland,
http://ic.epfl.ch/privacy-surveillance

64. بن إمرسون (23 سبتمبر 2014). الجمعية العامة للأمم المتحدة في دورتها الـ69. «تقرير المقرّر الخاص بشأن نشر وحماية حقوق الإنسان والحريّات الأساسيّة أثناء مكافحة الإرهاب».
https://docs.google.com/document/d/18U1aHmKx9jfDQjCZeAUYZdRjl6iF4QjuS_aJO2Uy7NY/edit?pli=1.

65. كيم زيتر (22 أكتوبر 2013). مجلة وايرد. مقال: «محكمة تقضي بضرورة الحصول على إذن مستند إلى وجود مشتبه فيه محتمل، لتفعيل مجسّات الـ«جي بي إس»».

Wired,
http://www.wired.com/2013/10/warrant-required-gps-trackers.

66. روبرت بارنز (25 يونيو 2014). صحيفة واشنطن بوست. مقال: «المحكمة العليا تلزم الشرطة الحصول على مذكّرات قضائيّة في معظم أحوال تفتيش الخلوي».

Washington Post,
http://www.washingtonpost.com/national/supreme-court-police-must-get-warrants-for-most-cellphonesearches/2014/06/25/e2ff1326-fc6b-11e3-8176-f2c941cf35f1_story.html.

67. أورين كير وغريغ نجيم (1 أغسطس 2012). مجلة إيه بي إيه. مقال: «مسألة البيانات: هل يجب إعادة النظر في نظام الطرف الثالث؟».
http://www.abajournal.com/magazine/article/the_data_question_should_the_third-party_records_doctrine_be_revisited.

ريتشارد م. تومبسون الثاني (5 يونيو 2014). «خدمة بحوث الكونغرس». تقرير: «التعديل الرابع في الدستور ونظام الطرف الثالث».

Congressional Research Service,
http://fas.org/sgp/crs/misc/R43586.pdf

68. حاضراً، فإنّ القاضية [سونيا] سوتومايور هي الوحيد في «المحكمة العليا» التي كتبت تأييداً لإدخال تلك التعديلات. ريتشارد م. تومبسون الثاني (5 يونيو 2014). «خدمة بحوث الكونغرس». تقرير: «التعديل الرابع في الدستور ونظام الطرف الثالث».

Congressional Research Service,
http://fas.org/sgp/crs/misc/R43586.pdf

69. في 2014، استخدم الروس إحدى ثغرات «اليوم- صفر» في نظام «ويندوز» كي يتجسّسوا على حلف الـ«ناتو» والحكومة الأوكرانيّة. آلين ناكاشيما (13 أكتوبر 2014). صحيفة واشنطن بوست. مقال: «استخدم «هاكرز» روس ثغرات «اليوم- صفر» للاختراق الـ«ناتو» وأوكرانيا، ضمن حملة تجسّس سبراني».
Washington Post,

http://www.washingtonpost.com/world/national-security/russian-hackers-use-zero-day-to-hack-nato-ukraine-in-cyberspy-campaign/2014/10/13/f2452976-52f9-11e4-892e-602188e70e9c_story.html

70. كوري دوكتورو (11 مارس 2014). صحيفة الغارديان. مقال: «إذا أرادت «القيادة الحكوميّة للاتّصالات» تحسين الأمن القومي، يجب عليها إصلاح تقنيّاتنا».

Guardian,

http://www.theguardian.com/technology/2014/mar/11/gchq-national-security-technology.

Dan Geer (2013), «Three policies,»

http://geer.tinho.net/three.policies.2013Apr03Wed.PDF

71. ديفيد ي. سانغر (29 أبريل 2014). صحيفة نيويورك تايمس. مقال: «البيت الأبيض يشرح تفكيره بشأن الاختلالات في الأمن السبراني».

New York Times,

http://www.nytimes.com/2014/04/29/us/white-house-details-thinking-on-cybersecurity-gaps.html.

72. كانت تلك التوصية رقم 30 من تلك اللجنة. ريتشارد كلارك وآخرون (12 ديسمبر 2013)، «الحريّة والأمن في عالم متغيّر: تقرير وتوصيات «لجنة الرئاسة للمراجعة بشأن الاستخبارات وتقنيات الاتصالات»»، المكتب التنفيذي للرئيس الأميركي، ص 187.

http://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf.

73. بروس شناير (19 مايو 2014). صحيفة آتلانتيك. مقال: «هل يجب على الـ«هاكرز» الأميركيّين إصلاح ثغرات الأمن السبراني أم الاستفادة منها؟».

Atlantic,

http://www.theatlantic.com/technology/archive/2014/05/should-hackers-fix-cybersecurity-holes-or-exploitthem/371197.

74. ميتشل دانيال (28 أبريل 2014). المدوّنة الإلكترونيّة للبيت الأبيض. مقال: «ثغرة «هارت بليد»: شرح عن سياق الكشف عن ثغرات سبرانيّة».

White House Blog,

http://www.whitehouse.gov/blog/2014/04/28/heartbleed-understanding-when-we-disclose-cyber-vulnerabilities.

ديفيد ي. سانغر (29 أبريل 2014). صحيفة نيويورك تايمس. مقال: «البيت الأبيض يشرح تفكيره بشأن الاختلالات في الأمن السبراني».

New York Times,

http://www.nytimes.com/2014/04/29/us/white-house-details-thinking-on-cybersecurity-gaps.html.

كريستوفر جوي (8 مايو 2014). صحيفة استراليان فايننشال ريفيو. مقال: «نص مقابلة: الرئيس السابق لـ«وكالة الأمن القومي» وقائد «القيادة السبرانيّة الأميركيّة»، الجنرال كيث آلكسندر».

Australian Financial Review,

http://www.afr.com/Page/Uuid/b67d7b3e-d570-11e3-90e8-355a30324c5f.

75. بروس شناير (5 سبتمبر 2013). صحيفة الغارديان. مقال: «الحكومة الأميركيّة خانت الإنترنت. نحتاج إلى استرداد ثقتها».

Guardian,

http://www.theguardian.com/commentisfree/2013/sep/05/government-betrayed-internet-nsa-spying

ستيفان فاريل (2013). مقال: «الرقابة الواسعة هي هجوم سبراني».

http://tools.ietf.org/pdf/draft-farrellperpass-attack-00.pdf.

76. شارلي سافاج (27 سبتمبر 2010). صحيفة نيويورك تايمس. مقال: «الولايات المتحدة تحاول تسهيل التنصّت على الإنترنت».

New York Times,
http://www.nytimes.com/2010/09/27/us/27wiretap.html

رايان سنغل (17 فبراير 2011). مجلة وايرد. مقال: «الـ«إف بي آي» تضغط لفرض «أبواب خلفيّة» للرقابة في أدوات «ويب 2.0»».

Wired,
http://www.wired.com/2011/02/fbi-backdoors

فاليري كابروني (17 فبراير 2011). «خطاب أمام اللجنة الفرعيّة في مجلس النواب، للجريمة والإرهاب والأمن الوطني».

http://www.fbi.gov/news/testimony/going-dark-lawful-electronic-surveillance-in-the-face-of-new-technologies

77. ليس أمراً جديداً. ففي ثمانينيات القرن العشرين وتسعينياته، كانت «وكالة الأمن القومي» تدسّ «أبواباً خلفيّة» في شيفرة منتجات إلكترونيّة تبيعها شركة «كريبتو إيه. جي» السويسريّة. سكوت شاين وتوم بومان (4 ديسمبر 1995). صحيفة بالتيمور صن. مقال: «تخريب اللعبة».

http://cryptome.org/jya/nsa-sun.htm.

78. كريستوفر كِتشام (27 سبتمبر 2008). موقع «كاونتر بنش». مقال: «حصان طروادة إسرائيلي».

Counterpunch,
http://www.counterpunch.org/2008/09/27/an-israeli-trojanhorse

جيمس بامفورد (3 أبريل 2012). مجلة وايرد. مقال: «شركات شبحيّة مرتبطة بإسرائيل تتجسّس على أميركا لمصلحة إسرائيل».

Wired,
http://www.wired.com/2012/04/shady-companies-nsa/all.

ريتشارد ساندرز (ربيع 2012). موقع «برس فور كونفرسيشن». مقال: «شركات إسرائيليّة جاسوسة: «فرينت» و«ناروس»».

http://coat.ncf.ca/P4C/66/spy.pdf

79. في تسعينيات القرن العشرين، صدر عن «الأكاديميّات الوطنيّة» التوصيات عينها: التوصية 1- يجب ألا يمنع أي قانون، صنع وبيع واستعمال أي نوع من التشفير داخل الولايات المتحدة. بصورة محدّدة، إنّ وجود حظر تشريعي على استعمال تشفير مؤتمن عند طرف ثالث، سيؤدّي إلى إثارة مشاكل تقنيّة وقانونيّة ودستوريّة. تقنيّاً، هناك سبُل عدّة للالتفاف على حظر كذلك. وقانونيّاً، هناك مشكلات دستوريّة، خصوصاً ما تعلّق بحرية التعبير، سوف تثار بشكل مؤكّد؛ وهي مشكلات ليست هيّنة الحل. صيغت التوصية كي تدعم على وجه الخصوص، ذلك الجانب من سياسة الإدارة بشأن كتابة التشفير». كنيث دبليو. دام وهيربرت س. لين (1995): «مطبعة الكليّات الوطنيّة». كتاب: **دور التشفير في حماية مجتمع المعلومات**.

http://www.nap.edu/catalog.php?record_id=5131.

80. بروس شناير (4 أكتوبر 2014). شبكة «سي آن آن». مقال: «أوقفوا الهستيريا بشأن تشفير «آبل»».

CNN,
http://edition.cnn.com/2014/10/03/opinion/schneier-apple-encryption-hysteria/index.html

81. «المكتب التنفيذي للمحاكم الأميركيّة» (11 يونيو 2014). تقرير: «الجدول 3: الاعتداءات الكبرى التي أوجبت إعطاء أذن قضائي بالتعرّض، وفقاً «18 «يو إس سي» 2519»، من بداية يناير إلى نهاية ديسمبر للعام 2013».
http://www.uscourts.gov/Statistics/WiretapReports/wiretap-report-2013.aspx.

82. آندي غرينبرغ (2 يوليو 2014). مجلة وايرد. «صعود ظاهرة التشفير، أدّى إلى تضليل الشرطة 9 مرات في 2013، وهو رقم قياسي».

Wired,
http://www.wired.com/2014/07/rising-use-of-encryption-foiled-the-cops-a-record-9-times-in-2013

83. ستيفن بلوفين (6-7 يونيو 2013). «مؤتمر قانونيّي الخصوصيّة»، بيركلي. ورقة بحث: «الاختراق الأخلاقي للكومبيوتر: استغلال الثغرات الموجودة في التنصّت على الإنترنت».
http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2312107

84. جاكوب آبلباوم (23 أكتوبر 2013). صحيفة دير شبيغيل. مقال: «برلين تشكو هل تجسّست أميركا على هاتف المستشارة ميركل؟».
Der Spiegel,
http://www.spiegel.de/international/world/merkel-calls-obama-over-suspicions-us-tappedher-mobile-phone-a-929642.html

أيان تراينور وفيليب أولترمان وبول لويس (23 أكتوبر 2013). صحيفة الغارديان. مقال: «أنغيلا ميركل تهاتف أوباما: هل تتجسّس على هاتفي الخلوي؟».
Guardian,
http://www.theguardian.com/world/2013/oct/23/us-monitored-angelamerkel-german.

85. إيوين ماكآسكل وجوليان بورغر (30 يونيو 2013). صحيفة الغارديان. مقال: «تسريبات جديدة عن «وكالة الأمن القومي» تُظهر تجسّسها على حلفاء أوروبيّين».
Guardian,
http://www.theguardian.com/world/2013/jun/30/nsa-leaks-us-bugging-european-allies.

غلين غرينوالد (2014). كتاب لا مكان للاختباء: إدوارد سنودن و«وكالة الأمن القومي» وحال الرقابة في الولايات المتحدة. (دار ماكميليان للنشر).
http://leaksource.info/2014/07/31/glenn-greenwalds-no-place-to-hide-nsa-documents-excerpts

86. لورا بواتراس ومارسيل روزنباخ وهولغر ستارك (26 أغسطس 2013). صحيفة دير شبيغيل، مقال: «الاسم الشيفري هو «آبالاتشي»: كيف تجسّست أميركا على أوروبا والأمم المتحدة».
Der Spiegel,
http://www.spiegel.de/international/world/secret-nsa-documents-showhow-the-us-spies-on-europe-and-the-un-a-918625.html

87. وجود حالات من عدم التيقن في المساحة بين الاستفادة والهجوم، قد يؤدّي إلى تصاعد غير مرغوب فيه للتوتر. هربرت لين (خريف 2012). «دراسات استراتيجيّة». دراسة: «آليّات تصعيد الصراع وإنهائه في الفضاء السبراني».
Strategic Studies Quarterly 6,
http://www.au.af.mil/au/ssq/2012/fall/lin.pdf.

88. بيتر كراسكا (يناير 2007). مجلة بوليس. مقال: «العسكرة وأعمال الشرطة: دلالتهما بالنسبة لشرطة القرن 21».
Policing 1,
http://cjmasters.eku.edu/sites/cjmasters.eku.edu/files/21stmilitarization.pdf.

آبيغيل هال وكريستوفر كوينه (ربيع 2013). مجلة اندبندنت ريفيو. تقرير: «عسكرة الشرطة المحلي في الولايات المتحدة».
Independent Review 17,
http://www.independent.org/pdf/tir/tir_17_04_01_hall.pdf

ماثيو ويتس (مارس 2013). مجلة دراسات 9/11. مقال: «أكثر تصميماً من أورويل: ظاهرة العسكرة الرديفة في الولايات المتحدة بعد 9/11».
Journal of 9/11 Studies 36,
http://www.journalof911studies.com/resources/2013WittVol36Mar.pdf

89. من الممكن البدء بقراءة كتاب جيّد عن تلك المواضيع. رايدلي بالكو (2013). بابليك آفيرز برس. «صعود الشرطة المحاربة: عسكرة قوات الشرطة الأميركية».

http://books.google.com/books?id=M3KSMQEACAAJ

90. باراك أوباما (17 يناير 2014). صحيفة واشنطن بوست. مقال: «مقتطفات من خطاب الرئيس أوباما عن إصلاح «وكالة الأمن القومي»».

Washington Post,
http://www.washingtonpost.com/politics/full-text-of-president-obamas-jan-17-speech-on-nsa-reforms/2014/01/17/fa33590a-7f8c-11e3-9556-4a4bf7bcbd84_story.html.

91. سكوت شارني (30 أبريل 2010). شركة مايكروسوفت. تقرير: «إعادة التفكير في التهديد السبراني: إطار للعمل والتحرّك قدماً».

Microsoft Corporation,
http://www.microsoft.com/en-us/download/details.aspx?id=747

92. هناك كتابات عن إمحاء الفاصل بين الجرائم وأعمال الحرب. بنجامين ب. بريستر (24 أغسطس 2007). كلية القانون في جامعة فلوريدا.

http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1009845

93. بات كثيرون يستخدمون ذلك المصطلح المشحون بالعواطف. ريتشارد بيهر (13 أكتوبر 2008). شبكة «فوكس نيوز». مقال: «أزمة غير مسبوقة تضع «البنك الدولي» تحت حصار سبراني».

FOX News,
http://www.foxnews.com/story/2008/10/13/world-bank-under-cyber-siege-in-unprecedented-crisis.

مؤسّسة «كاسبارسكي لاب» (2014). «منتدى شركة كاسبرسكي للأمن الحكومي». تقرير: «ماذا تفعل أميركا إذا وقعت تحت حصار سبراني؟».

Kaspersky Government Cybersecurity Forum,
http://kasperskygovforum.com.

94. هناك اقتراح بإنشاء نوع من «التجنيد الإلزامي السبراني» بهدف تعبئة الشبكات في حال اندلاع حرب سبرانيّة. سوزان برنر وليو كلارك (أكتوبر 2010). فاندربيلت جورنال أوف ترانزشونال لو. مقال: «المدنيّون أثناء عمليات الحرب السبرانيّة: متطوّعون».

Vanderbilt Journal of Transnational Law 43,
http://www.vanderbilt.edu/jotl/manage/wp-content/uploads/Brenner-_Final_1.pdf.

95. «مؤسّسة راند» (20 مارس 2001). تقرير: «عرض عام لـ«قانون بوزيه كوميتاتوس»».

http://www.rand.org/content/dam/rand/pubs/monograph_reports/MR1251/MR1251.AppD.pdf

شارلز دويل وجنيفر إلسي (16 أغسطس 2012). خدمة بحوث الكونغرس. «عن «قانون بوزيه كوميتاتوس» وأمور متّصلة به: استعمال العسكري لتنفيذ القانون المدني».

Congressional Research Service,
http://www.fas.org/sgp/crs/natsec/R42659.pdf

96. ريهت أ. هرنانديز (أكتوبر 2012). مجلة آرمي. مقال: «عن «القيادة السبرانيّة الأميركيّة»: الفضاء السبراني مساحة عمل لقوة أميركيّة حاسمة».

Army,
http://connection.ebscohost.com/c/articles/82115370/u-s-army-cyber-commandcyberspace-americas-force-decisive-action.

97. في العقود الأخيرة، بذلت «وكالة الأمن القومي» جهداً أكبر في إمداد الشركات الأميركيّة الخاصة بالبيانات، إضافة إلى حماية الاتّصالات. تحتاج الشركات إلى عون الحكومة، لكنها تحتاج أن يجري ذلك بعلانية أكبر. سوزان لانداو (29 سبتمبر 2014). جورنال أوف ناشيونال سكيورتي لو أند بوليسي. مقال: «تحت الرادار: جهود «وكالة الأمن القومي» في حماية البنية التحتيّة للقطاع الخاص في الاتصالات».

Journal of National Security Law and Policy,
http://jnslp.com/2014/09/29/under-the-radar-nsas-efforts-to-secure-private-sector-telecommunications-infrastructure

98. روبـرت أ. روي (11 يونيـو 1987). مجلس النـواب، لجنة العلوم والفضاء والتكنولوجيـا. مقال: «تقرير عن «قانون أمن الكومبيوتر- 1987»».
https://beta.congress.gov/congressional-report/107th-congress/senate-report/239/1.
«مركز معلومات الخصوصيّة الإلكترونيّة» (2014). تقرير: «قانون أمن الكومبيوتر- 1987».
http://epic.org/crypto/csa.

99. مولتـن مولـر (21 يونيـو 2012). «مشروع حوكمة الإنترنـت». تقرير: «تحليل المخاطـر في «المجلس العالمي للمعلوماتية والاتصالات»- القسم4: «وحدة المعلوماتيّة والاتصالات» والأمن السبراني».
Internet Governance Project,
http://www.internetgovernance.org/2012/06/21/threat-analysis-of-the-wcit-4-cybersecurity.

100. ذهبـت حكومة البرازيل إلى حدّ اقتراح قانون بذلك الشـأن، لكنه لم يقر. إسـتبان إسرائيـل وأنثوني بودل (28 أكتوبر 2013). وكالة رويترز للأنباء. مقال: «البرازيل تصرّ على تخزين بيانات الإنترنت محليّاً، بعد انكشـاف التجسّس الأميركي».
Reuters,
http://www.reuters.com/article/2013/10/28/net-us-brazil-internet-idUSBRE99R10Q20131028.
Anthony Boadle (18 Mar 2014), «Brazil to drop local data storage rule in Internet bill,

101. ميشـال برينباوم (1 نوفمبر 2013). صحيفة واشـنطن بوسـت. مقـال: «ألمانيا تتطلّـع للاحتفاظ ببيانات الإنترنت المحلي وبريدها الإلكتروني، داخل حدودها».
Washington Post,
http://www.washingtonpost.com/world/europe/germany-looks-at-keeping-its-internet-e-mail-trafficinside-its-borders/2013/10/31/981104fe-424f-11e3-a751-f032898f2dbc_story.html.

102. شـارلزماينز (11 يوليو 2014). إذاعة دويتشـه فيلله. مقال: «روسـيا تزيد صلابة الإنترنت بواسـطة قانون الخوادم».
Deutsche Welle,
http://www.dw.de/russia-tightensinternet-screws-with-server-law/a-17779072
ادريـان هينـي (12 يوليو 2014). مجلة إيسـت- وسـت ديجيتال نيوز. مقـال: «قوانين جديـدة لتخزين المعلومات تؤثّر في لاعبين محليّين وأجانب- لكن لا يوجد «سور صيني» حول روسيا».
East-West Digital News,
http://www.ewdn.com/2014/07/12/new-personal-data-storage-rules-to-affect-both-foreign-and-domestic-players-but-no-chinese-wall-surrounding-russia

103. جاكلين بوركل (2 يناير 2014). مقال: «هل «فيسبوك» فضاء عام أو خاص؟».
http://www.tandfonline.com/doi/abs/10.1080/1369118X.2013.870591.

104. حتـى لـو فعلنا، لكنّا وجدنـا أنّها اتفاقيّة غائمة، وتعطـي الشركة الحق في فعل ما يحلو لهـا... بل وتغيير تلك الاتفاقيّة وفق إرادتها، من دون إشعارنا ولا الحصول على موافقتنا.

105. سكوت ليبارجر (1999). مقال: «قناة أم منتدى: مجازات قانونيّة من أجل الإنترنت».
http://www.tandfonline.com/doi/abs/10.1080/08997225.1999.10556239.

106. نـواه د. زاتـز (خريف 1998). مجلة هارفرد للقانون والتكنولوجيـا. مقال: «أرصفة في الفضاء الافتراضي: إفساح المجال للمنتديات العامة في البيئة الإلكترونيّة».

12,
http://jolt.law.harvard.edu/articles/pdf/v12/12HarvJLTech149.pdf.

ليريسا ليدسكي (ديسمبر 2011). مجلة جامعة بوسطن للقانون. مقال: «منتدى عمومي 2.0».
http://www.bu.edu/law/central/jd/organizations/journals/bulr/volume91n6/documents/LIDSKY.pdf

الفصل 14: حلول للشركات

1. الأرجح أننا سـنتمكن من ابتكار مـا يخرجنا من الكارثة الإيكولوجيّة التي يمثّلهـا التغيّر المناخي، ولن نحتفظ بطريقتنـا حـاضراً في التعامل معها. بيـورن لومبورغ (2001). «مطبعـة جامعة كامـبردج». كتاب: **البيئي المتشكّك: قياس حال العالم فعليّاً.**

https://encrypted.google.com/books?id=JuLko8USApwC

2. «منظّمـة التنميـة والتعـاون الاقتصـادي» (2013). وثيقة: «إطـار الخصوصيّة- «منظّمة التنميـة والتعاون الاقتصادي»».

http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf.

3. البرلـان الأوروبـي و«مجلس أوروبـا» (24 أكتوبر 1995). وثيقـة: «قانون من البرلـان الأوروبي و«مجلس أوروبـا» في 24 أكتوبر 1995، بشـأن حمايـة الأفراد في ما يتّصل بالتعامل مع المعلومات الشـخصيّة والتحرك الحر لتلك المعلومات».

http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML

نيل روبنسون (2009). «مؤسّسة راند». دراسة: «مراجعة القانون الأوروبي لحماية المعلومات».
RAND Corporation,
http://ico.org.uk/~/media/documents/library/data_protection/detailed_specialist_guides/review_of_eu_dp_directive.ashx

4. كارلـين ليلينغتون (14 مايو 2014). صحيفة أيريش تايمس. مقال: «تحليل: «غوغل» يتلقى ضربة جديدة بقوانين «الاتحاد الأوروبي» للخصوصيّة».

Irish Times,
http://www.irishtimes.com/business/sectors/technology/analysis-google-takes-another-hit-with-eu-privacy-rulings-1.1793749

«مؤسّسـة برايس ووتر هاوس كوبـرز» (يوليو 2014). تقرير: «إصلاحات «الاتحاد الأوروبي» بشـأن حماية البيانات: تحدّيات للأعمال».

http://www.pwc.com/en_US/us/risk-assurance-services/publications/assets/pwc-eu-data-protection-reform.pdf.

5. المفوضيّة الأوروبيّة (25 يناير 2012). تقرير: «المفوضيّة تقترح إصلاحاً شاملاً لقوانين حماية الخصوصيّة».
http://ec.europa.eu/justice/newsroom/data-protection/news/120125_en.htm.

«المفوضيّـة الأوروبيّة» (12 مارس 2014). تقرير: «التقدّم في قانون «الاتحاد الأوروبي» لحماية البيانات الذي صار غير قابل للتراجع عنه، عقب تصويت في البرلمان الأوروبي».

http://europa.eu/rapid/press-release_MEMO-14-186_en.htm.

6. «منظّمة التنمية والتعاون الاقتصادي» (2013) تقرير: «إطار الخصوصيّة في المنظّمة».

http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf.

7. يصلح المقال التالي مدخلًا لفهم اقتصاديّات خصوصيّة البيانات. تايلر موور (2011). منشـورات «ناشـيونال أكاديمي برس». مقال: «مدخل إلى اقتصاديّات الأمن السبراني: المبادئ وخيارات السياسة».

http://cs.brown.edu/courses/csci1800/sources/lec27/Moore.pdf.

8. تتزايد الاعتداءات والاختراقات بالنسبة لبيانات الرعاية الصحيّة أميركيّاً، مع ما يرافق ذلك من غرامات. باتريك أوتول وكوري دنيس ودوغلاس ليفي (28 مارس 2014). مقال: «أفضل الممارسات لتجنّب المسؤوليّة القانونيّة عن التعدي على البيانات».
http://milawyersweekly.com/news/2014/03/28/commentarybest-practices-for-avoiding-data-breach-liability

9. ساشا رومانوسكي وديفيد هوفمان واليساندرو أكويستي (25-26 يونيو 2012). «المنتدى السنوي اقتصاديّات أمن المعلومات»، برلين (ألمانيا). دراسة: «تحليل تجريبي للمنازعات القضائيّة بشأن اختراق البيانات».
Annual Workshop on the Economics of Information Security, Berlin, Germany,
http://weis2012.econinfosec.org/papers/Romanosky_WEIS2012.pdf.

10. تدافع شركة «تارغت» عن نفسها في مجموعة دعاوى قضائيّة ترتّبت على اختراق البيانات عندها في 2013. أليكس ويليامز (23 ديسمبر 2013). موقع «تيك كرانش». مقال: «ربّما تغرّم شركة «تارغت» 36 بليون دولار جزاءً لاختراق بيانات بطاقات ائتمان لديها».
Tech Crunch,
http://techcrunch.com/2013/12/23/target-may-be-liable-for-up-to-3-6-billion-from-creditcard-data-breach
لانس ديروني (3 أبريل 2014). مقال: «المجلس القضائي للمنازعات المتعددة» يمركز الدعاوى ضد «تارغت» في «منيسوتا»».
http://www.law360.com/articles/524968/jpml-centralizestarget-data-breach-suits-in-minn

11. برايان كريبس (8 يناير 2014). مدوّنة إلكترونيّة. مقال: «شركات تقاضي بنكاً بعد إفلاسها بسبب عملية سطو سبراني».
Krebs on Security,
http://krebsonsecurity.com/2014/01/firm-bankrupted-by-cyberheist-sues-bank
برايان كريبس (13 أغسطس 2014). مدوّنة إلكترونيّة. مقال: «شركة في ولاية «تينسي» تقاضي بنكاً لتغريمه 37 ألف دولار، بعد عملية سطو سبراني».
Krebs on Security,
http://krebsonsecurity.com/2014/08/tenn-utility-sues-bank-over-327k-cyberheist

12. المقال التالي يحمل اقتراحاً بهذا الشأن. موريزيو نالدي ومارتا فلاميني وغويزيبي دا آكويستو (2013). مطبعة «سبرينغر». كتاب: **الشبكة وأمن النظام**. نص: «المسؤوليّة القانونيّة عن اختراق البيانات: اقتراح مقاربة تعتمد على ربط العقوبة بالدخل».
http://link.springer.com/chapter/10.1007%2F978-3-642-38631-2_20.

13. ويليس هير وآخرون (يوليو 1973). وزارة الصحة. تقرير: «سجلات، كومبيوترات وحقوق مواطنين: تقرير إلى اللجنة الاستشاريّة للوزير عن النُظُم المؤتمتة للمعلومات الشخصيّة».
US Department of Health, Education and Welfare,
http://www.justice.gov/sites/default/files/opcl/docs/rec-com-rights.pdf

14. كُتِبَ الكثير عن طرق استفادة قوانين الخصوصيّة من تشريعات البيئة. دينس د. هيرش (خريف 2006). مجلة **جورجيا لو ريفيو**. مقال: «حماية البيئة الداخليّة: ماذا تستطيع تشريعات الخصوصيّة تعلّمه من قانون البيئة».
Georgia Law Review 41,
http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1021623
إيرا س. روبنشتاين (2011). دراسة: «الخصوصيّة والابتكار التشريعي: الخروج من الأعراف الطوعيّة».
http://www.ftc.gov/sites/default/files/documents/public_comments/privacy-roundtables-comment-projectno.p095416-544506-00022/544506-00022.pdf.

15. ربما برزت الحاجة إلى شيء من الاستثناء للبرمجيّات المجانيّة والمفتوحة المصدر، وكذلك الحالات التي لم يوقّع المستخدم فيها عقداً مع الشركة البائعة للبرمجيّات.

16. غويسبي داري- ماتياشي ونوينو غاروبا (مايو 2009). مجلة **جورنال أوف لو، أيكونوميكس أند أورغنايزايشن**. مقال: «التجنّب الأقل كلفة: مأساة الأمان العام».
Journal of Law, Economics, and Organization 25,
http://papers.ssrn.com/sol3/papers.cfm?abstract_id=560062.
بول روزنزفايغ (5 نوفمبر 2013). مجلة **لوفير**. مقال: «الأمن السبراني والمتجنّب بالكلفة الأقل».
Lawfare,
http://www.lawfareblog.com/2013/11/cybersecurity-and-the-least-costavoider

17. الحق أنّ مفهوم ملكيّة البيانات معقّد تماماً. علي الخوري (نوفمبر 2012). مقال: «ملكيّة المعلومات: من يملك «بياناتي»؟».
http://www.id.gov.ae/assets/FNukwmhbQ4k.pdf.aspx
جاكوب فيكتور (نوفمبر 2013). تقرير: ««قانون «الاتحاد الأوروبي» عن حماية البيانات العامة: نحو نظام مناسب في حماية خصوصيّة المعلومات».
http://www.yalelawjournal.org/comment/the-eu-general-data-protection-regulation-toward-a-property-regime-for-protecting-data-privacy

18. جنيفر فالنتينو- دي فرايز وجيرمي سينغر- فاين (7 ديسمبر 2012). صحيفة **وول ستريت جورنال**. مقال: «إنّهم يعرفون ماذا تتسوّقون».
Wall Street Journal,
http://online.wsj.com/news/articles/SB10001424127887324784404578143144132736214
جيرمي سينغر- فاين (7 ديسمبر 2012). صحيفة **وول ستريت جورنال**. مقال: «كيف تراقبك «داتايوم»».
http://blogs.wsj.com/digits/2012/12/07/how-dataium-watches-you.

19. فرانك باسكال (21 أبريل 2009). مقال: «الميل المقلق صوب تبني نظم التصنيف المستندة إلى السريّة التجاريّة».
http://www.chicagoip.com/pasquale.pdf.

20. إيثان زوكرمان (5 سبتمبر 2012). مقال: «لوائح «إدارة أمن النقل» للتدقيق قبل السفر بين العدالة وضبابيّة الخوارزميّات».

21. دانيال فايتزنر (29- 30 يناير 2014). «المنتدى الثاني في «ماساشوستس- كامبردج» عن الموثوقيّة: سياسة العلوم والتكنولوجيا». دراسة: «فلسفة القانون في الموثوقيّة».
2nd International Workshop on Accountability: Science, Technology and Policy, Cambridge, Massachusetts,
http://dig.csail.mit.edu/2014/AccountableSystems2014/abs/weitzner-account-jurisprudence-abs.pdf
إد فيلتن (12 سبتمبر 2012). موقع «فريدوم تو تينكر». مقال: «الخوارزميّات الموثوقة».
Freedom to Tinker,
https://freedom-to-tinker.com/blog/felten/accountable-algorithms

22. تشمل الأمثلة على ذلك شركة «مايكروسوفت» و«المنتدى الاقتصادي العالمي». كريغ موندي (مارس/ أبريل 2014). مجلة **فورين آفيرز**. مقال: «البراغماتية في الخصوصيّة: ركّز على استعمال المعلومات وليس تجميعها».
Foreign Affairs 93,
http://www.foreignaffairs.com/articles/140741/craig-mundie/privacy-pragmatism
ويليام هوفمان (مايو 2014). «المنتدى الاقتصادي العالمي». تقرير: «إعادة التفكير في المعلومات الشخصيّة: نظرة جديدة لتمتين الثقة».
World Economic Forum,
http://reports.weforum.org/rethinking-personal-data

فريــد كايت وبيــتر كولين وفيكتور ماير- شــوبنرغر (مايو 2014). «معهد أكســفورد للإنترنــت» في «جامعة أكســفورد». دراســة: «مبادئ حماية المعلومات في القــرن 21: إعادة النظر في الخطــوط التوجيهيّة لــ«منظّمة التنمية والتعاون الاقتصادي- 1980»».

Oxford Internet Institute, University of Oxford,
http://www.oii.ox.ac.uk/publications/Data_Protection_Principles_for_the_21st_Century.pdf

«مجلس مستشاري الرئيس عن العلوم والتكنولوجيا» (مايو 2014). تقرير: «البيانات الضخمة» والخصوصيّة: مقاربة تكنولوجيّة».

http://www.whitehouse.gov/sites/default/files/microsites/ostp/PCAST/pcast_big_data_and_privacy_-_may_2014.pdf.

23. كريــس غــاي هوفناغــل (2 ســبتمبر 2014). موقع «ســلايت». مقــال: «المخادعــة الإيحائيّــة في الخصوصيّة البراغماتيّة».

Slate,
http://www.slate.com/articles/technology/future_tense/2014/09/data_use_regulation_the_libertarian_push_behind_a_new_take_on_privacy.single.html

24. أ. ميخائيــل فرومكــين (23 فبرايــر 2014). جامعة ميامي. دراســة: «تنظيــم الرقابة العامــة بوصفها تلويثاً للخصوصيّة: دروس من القوانين عن الأثر البيئي».

University of Miami,
http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2400736

25. جولي بريل (2 يونيو 2014). «ورشــة مستشــاري «الاتحاد الأوروبي» لحماية المعلومات عن «حماية المستهلك والمنافسة في العصر الرقمي»، بروكسل، بلجيكا». دراسة: «نسج مفرش مزركش لحماية الخصوصيّة والمنافسة في عصر «البيانات الضخمة»».

http://www.ftc.gov/system/files/documents/public_statements/313311/140602edpsbrill2.pdf.

جولز بولونتســكي وعمر تينه (6 ديســمبر 2012). «فيوتشر برايفسي فوروم». تقرير: «ليســت المسألة حجم البيانات التي تحوزها، بل طريقة استعمالك لها».

Future of Privacy Forum,
http://www.futureofprivacy.org/wp-content/uploads/FPF-White-Paper-Its-Not-How-Much-Data-You-Have-But-How-You-Use-It_FINAL.pdf

26. «الاتحاد الأوروبي» (9 ديسمبر 2013). وثيقة: «السلطات الوطنيّة لحماية البيانات».
http://ec.europa.eu/justice/data-protection/bodies/authorities/index_en.htm

27. آلــون هاليفــي وبيــتر نورفيــج وفرنانــدو بيريــرا (مارس/أبريــل 2009). «معهــد المهندســين الكهربائيّين والإلكترونيّين: النُظُم الذكيّة 2.0». «الكفاءة غير المنطقيّة للبيانات».

https://static.googleusercontent.com/media/research.google.com/en/us/pubs/archive/35179.pdf

28. دووغ غروس (7 يناير 2013). شبكة «سي آن آن». مقال: «مكتبة الكونغرس» تنقّب في 170 بليون تغريدة».
CNN,
http://www.cnn.com/2013/01/07/tech/social-media/library-congress-twitter.

29. مارتن فاولر (12 ديسمبر 2013). «داتنشبارشزامكايت».
http://martinfowler.com/bliki/Datensparsamkeit.html.

30. بالطبــع، الحمايــات القانونيّة لا تتحوّل بالضرورة إلى حماية حقيقيّة. في 2011، اكتُشِــفَ أن الحكومة الألمانيّة تتجسّس على مواطنيها باستخدام برنامج خبيث من نوع «تروجان»، مخترقة بنفسها قوانينها القويّة في حماية البيانــات. وكما علمنا مراراً وتكــراراً، لا قانون بإمكانه أن يحمينا من حكومة ترفض الالتزام به. «نادي فوضى الكومبيوتر» (8 أكتوبر 2011). تقرير: «تحليل «نادي فوضى الكومبيوتر» لبرنامج حكومي خبيث».
Chaos Computer Club analyzesgovernment malware,»
http://ccc.de/en/updates/2011/staatstrojaner

31. دي. آل. إيه بايبر (7 مارس 2013). دراسة «قوانين حماية البيانات في العالم».
http://files.dlapiper.com/files/Uploads/Documents/Data_Protection_Laws_of_the_World_2013.pdf
ثيودور كوبوس الثالث وغونزالو زيبالوس (19 فبراير 2014). موقع «بايكر هوستلر». دراسة: «الوجيز العالمي في قوانين حماية خصوصيّة البيانات في 2014».
Baker Hostetler,
http://www.bakerlaw.com/files/Uploads/Documents/Data%20Breach%20documents/International-Compendium-of-Data-Privacy-Laws.pdf.

32. أستطيع الوصول إلى بعضها إذا فعّلت خاصيّة التسجيل الزمني للبحث. دايف غرينباوم (12 يوليو 2014). موقع «لايف هاكر». مقال: «أضاف «غوغل» صفحة لتاريخ عمليات البحث، تساعد على مزيد من التحكّم ببياناتك».
Life Hacker,
http://lifehacker.com/googles-newaccount-history-page-helps-further-control-1603125500

33. هيبو كامبوس (19 نوفمبر 2011). مدوّنة إلكترونيّة. «هيبو كامبوس يقاتل من أجل حقه في النفاذ إلى معلومات عن قلبه».
http://tedxtalks.ted.com/video/TEDxCambridge-Hugo-Campos-fight

34. بروس شناير (يوليو/ أغسطس). مقال: «تصنيف لبيانات الـ«سوشال ميديا»».
http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=5523874.

35. بلايك روز (13 سبتمبر 2011). موقع «فيسبوك». توجيه: «قائمة أصدقاء محسّنة».
Facebook,
https://www.facebook.com/notes/facebook/improvedfriend-lists/10150278932602131

36. توني برادلي (13 أكتوبر 2010). مجلة عالم الكومبيوتر. مقال: «أتظن أنّ تغريداتك خصوصيّة؟ فكّر ثانية».
PC World,
http://www.pcworld.com/article/207710/think_your_twitter_dm_is_private_think_again.html

37. ليسلي ميرديث (15 يناير 2013). شبكة «آن بي سي نيوز». مقال: «لماذا يجب عليك جعل حسابك على «أنستغرام» خصوصياً قبل يوم السبت؟».
NBC News,
http://www.nbcnews.com/tech/internet/why-you-should-make-instagram-private-saturday-f1B7987618

38. سيرجي مالينكوفيتش. صحيفة مختبر كاسبارسكي. مقال: «كيف تحمي خصوصيّتك على «بينترست».
Kaspersky Lab Daily,
http://blog.kaspersky.com/protect-your-privacy-on-pinterest.

39. «المكتب التنفيذي للرئاسة» (1 مايو 2014). تقرير: «البيانات الضخمة: التقاط الفرصة والحفاظ على القيم».
http://www.whitehouse.gov/sites/default/files/docs/big_data_privacy_report_may_1_2014.pdf.

40. يارون لانير (2013). دار «سايمون وشوستر». كتاب: من يملك المستقبل؟
Simon and Schuster,
http://books.google.com/books?id=w_LobtmRYmQC

41. «المكتب التنفيذي للرئاسة» (فبراير 2012). تقرير: «خصوصيّة بيانات المستهلك في عالم مترابط بالشبكات: إطار عمل لحماية الخصوصيّة وتحفيز الابتكار في الاقتصاد الرقمي العالمي».
http://www.whitehouse.gov/sites/default/files/privacy-final.pdf.

42. المفوضيّة الأوروبيّة (8 يوليو 2014). تقرير: «ورقة الحقائق عن تشريع «الحق في النسيان»».

http://ec.europa.eu/justice/data-protection/files/factsheets/factsheet_data_protection_en.pdf

43. روري سيلان- جونز (13 مايو 2014). هيئة الإذاعة البريطانيّة. مقال: «المحكمة الأوروبيّة تؤيّد «الحق في النسيان» في قضايا مرفوعة ضد «غوغل»».

BBC News,

http://www.bbc.com/news/world-europe-27388289.

44. جاين ويكفيلد (15 مايو 2014). هيئة الإذاعة البريطانيّة. مقال: «سياسيون ومحبو جنس الأطفال يطلبون من «غوغل» أن «يجري نسيانهم»».

BBC News,

http://www.bbc.com/news/technology-27423527.

45. أليساندرو مانتيليرو (يونيو 2013). تقرير: «اقتراح «الاتحاد الأوروبي» بصدد قانون عام لحماية البيانات، وجذور «الحق في النسيان»».

http://www.sciencedirect.com/science/article/pii/S0267364913000654.

46. أجريَت تجارب عدّة للبرهان على ذلك. باتريسيا نوربرغ ودانيال ر. هورني وديفيد أ. هورني (صيف 2007). مجلة جورنال أوف كونسيومر آفيرز. دراسة: «مفارقة الخصوصيّة: نوايا الكشف عن المعلومات الشخصية مقابل السلوكيّات».

Journal of Consumer Affairs 41,

http://onlinelibrary.wiley.com/doi/10.1111/j.1745-6606.2006.00070.x/abstract

سوزان ووترز وجيمس آكرمان (أكتوبر 2011). مجلة جورنال أوف كومبيوتر ميدييتد كوميونيكايشنز. دراسة: «استكشاف الخصوصيّة وإدارتها في «فيسبوك»: الدوافع والنتائج المتصوّرة المتّصلة بإشهار المعلومات طوعيّاً».

Journal of Computer-Mediated Communication 17,

http://onlinelibrary.wiley.com/doi/10.1111/j.1083-6101.2011.01559.x/full

أليساندرو آكويزتي، رالف كروس وفريد شتوتزمان (أبريل 2013). مجلة جورنال أوف برايفسي أند كونفيدنشاليتي. دراسة: «المُصغون الصامتون: تطوّر الخصوصيّة والإشهار على «فيسبوك»».

Facebook,» *Journal of Privacy and Confidentiality* 4,

https://www.cylab.cmu.edu/news_events/news/2013/acquisti-7-year-study-facebook-privacy.html

47. تبيّن أنّه من السهولة بمكان التلاعب بالناس كي ينسوا قلقهم بشأن الخصوصيّة. إدريس ادجيريد وآخرون (22 مارس 2013). دراسة: «براعات الخصوصيّة: التأطير، الكشوفات، وحدود الشفافيّة».

http://www.heinz.cmu.edu/~acquisti/papers/acquisti-sleights-privacy.pdf.

48. سارة م. واتسون (29 أبريل 2014). مقال: «إذا عرف المستهلكون كيف يستعملون بياناتهم، كيف يدعونها مريبة بعد ذلك؟».

http://blogs.hbr.org/2014/04/if-customers-knew-how-you-use-their-data-would-theycall-it-creepy.

49. كريس جاي هوفناغل وجان هافنغتون (28 فبراير 2014). مجلة لو ريفيو- جامعة كاليفورنيا. دراسة: «المجاني: جردة حساب لتكاليف السعر الأكثر شعبيّة على الإنترنت».

UCLA Law Review 61,

http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2235962.

50. كريتسن مارتن (2 ديسمبر 2013). مقال: «تكاليف التعاملات، الخصوصيّة، والثقة: الأهداف الحميدة والسقوط المتوقّع لسياسة الإشعار وخيار احترام الخصوصيّة على الإنترنت».

http://firstmonday.org/ojs/index.php/fm/article/view/4838/3802.

51. الأقرب إلى ما أعرف، أنّ تلك الفكرة اقترحها أستاذ حقوق بشكل مستقل. جيري كانغ (مارس 2012). بحث: «خصوصيّة الرقابة الذاتيّة».

http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1729332.

جاك م. بالكين (5 مارس 2014). بحث: «المرجعيّات الموثوقة معلوماتياً في العصر الرقمي».
http://balkin.blogspot.co.uk/2014/03/informationfiduciaries-in-digital-age.html.

52. جوناثان زيترين (1 يونيو 2014). موقع «نيو ريبابليك». مقال: «يستطيع «فيسبوك» أن يحسم الانتخابات من دون أن يلاحظه أحد».

New Republic,
http://www.newrepublic.com/article/117878/information-fiduciary-solution-facebook-digital-gerrymandering

53. دان غير (9 أكتوبر 2013). «مبادلات في الأمن السبراني».
http://geer.tinho.net/geer.uncc.9x13.txt

54. اعتذر مبتكر الإعلانات الصغيرة التي تقفز على شاشة الحاسوب من دون استئذان [«بوب اب آدس»] عما فعله. إيثان زوكرمان (14 أغسطس 2014). مجلة آتلانتيك. مقال: «الخطيئة الأصيلة للإنترنت».

Atlantic,
http://www.theatlantic.com/technology/archive/2014/08/advertising-is-the-internets-original-sin/376041.

55. آن كافوكيان (يناير 2011). مقال: «الخصوصيّة بالتصميم: المبادئ التأسيسيّة السبعة».
http://www.privacybydesign.ca/content/uploads/2009/08/7foundationalprinciples.pdf.

«لجنة التجارة الفيدرالية» (مارس 2012). تقرير: «حماية خصوصيّة المستهلك في زمن التغيّر السريع: توصيات إلى رجال الأعمال وصُنّاع السياسة».
http://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf.

56. أنغريد لوندين (30 سبتمبر 2013). موقع «تيك كرانش». تقرير: «تشكل الإعلانات الرقمية 22 % من إجمالي إنفاق أميركا على الإعلانات في 2013، وإعلانات الهواتف النقّالة 3.7 %، فيما الإنفاق العالمي على الإعلانات يقارب 503 بليون دولار».

Tech Crunch,
http://techcrunch.com/2013/09/30/digital-ads-will-be-22-ofall-u-s-ad-spend-in-2013-mobile-ads-3-7-total-gobal-ad-spend-in-2013-503b-sayszenithoptimedia

الرسوم البيانيّة للتسويق (23 ديسمبر 2013). تقرير: «الغوص في البيانات: عن تأثير الإعلانات التلفزيونيّة في الولايات المتحدة».
http://www.marketingcharts.com/wp/television/data-dive-us-tv-ad-spend-and-influence-22524.

57. جيمس كانستلر (21 أكتوبر 2005). موقع «رايز زي هامر». مقال: «سيكولوجيّة الاستثمار السابق».
http://www.raisethehammer.org/article/181.

58. شارلي سافاج (14 مايو 2014). صحيفة نيويورك تايمس. مقال: «وفق أوراق كُشِفَت أخيراً، شركات للهواتف قاومت «وكالة الأمن القومي» في المحاكم».

New York Times,
http://www.nytimes.com/2014/05/15/us/politics/phone-company-pushed-back-against-nsasdata-collection-court-papers-show.html

كلير كاين ميللر (13 يونيو 2013). صحيفة نيويورك تايمس. مقال: «قرار سري لمحكمة يضع شركات التكنولوجيا في قيود البيانات».

New York Times,
http://www.nytimes.com/2013/06/14/technology/secret-court-ruling-put-tech-companies-in-databind.html.

59. إيوين ماكآسكل (9 سبتمبر 2013). صحيفة الغارديان. مقال: «قضية من «ياهوو» ضد طلبات «وكالة الأمن القومي» لبيانات المستخدم».
Guardian,
http://www.theguardian.com/world/2013/sep/09/yahoo-lawsuit-nsa-surveillance-requests

مايك مازنيك (27 يناير 2014). موقع «تيك ديرت». مقال: «تسوية بين السلطات الفيدراليّة وشركات الإنترنت تقضي بأن لا تسلم الأخيرة إلا أقل مما يكفي من المعلومات عن جهود الرقابة».
Tech Dirt,
https://www.techdirt.com/articles/20140127/17253826014/feds-reach-settlement-with-internet-companiesallowing-them-to-report-not-nearly-enough-details-surveillance-efforts.shtml.

سبنسر إكرمان (3 فبراير 2014). صحيفة الغارديان. مقال: «مايكروسوفت، «فيسبوك»، «غوغل»، و«ياهوو» تنشر طلبات أرسلتها «وكالة الأمن القومي»».
Guardian,
http://www.theguardian.com/world/2014/feb/03/microsoft-facebook-google-yahoo-fisa-surveillance-requests

60. «غوغل» (2014). «تقرير الشفافية».
https://www.google.com/transparencyreport/userdatarequests/US.

61. برايـان فانغ (9 يناير 2014). صحيفة واشـنطن بوسـت. مقال: «أول شركة اتصـالات هاتفيّة تنشر تقرير شفافيّة، لم تكن «إيه تي أند تي» أو «فريزون»».
Washington Post,
http://www.washingtonpost.com/blogs/the-switch/wp/2014/01/09/the-first-phonecompany-to-publish-a-transparency-report-isnt-att-or-verizon.

62. «فريزون» (22 يناير 2014). «تقرير شفافية من «فريزون»».
http://transparency.verizon.com/us-data.

63. غلـين غرينوالـد (5 يونيو 2013). صحيفة الغارديان. «تجمع «وكالة الأمن القومي» سـجلات هواتف الملايين من زبائن شركة «فريزون» يوميّاً».
Guardian,
http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order

64. كريغ تيمبرغ (1 مايو 2014). صحيفة واشنطن بوست. مقال: «آبل»، «فيسبوك»، وغيرهما تتحدّى الحكومة بإبلاغ المستخدم عن طلبات سريّة للبيانات».
http://www.washingtonpost.com/business/technology/apple-facebook-others-defyauthorities-increasingly-notify-users-of-secret-data-demands-after-snowden-revelations/2014/05/01/b41539c6-cfd1-11e3-b812-0c92213941f4_story.html

65. جاكـوب سـيغال (30 أغسـطس 2013). مقـال: «مايكروسـوفت» و«غوغـل» تتحالفان لمقاضـاة الحكومة الفيدرالية بشأن تجسّس «وكالة الأمن القومي».
http://bgr.com/2013/08/30/microsoft-google-nsa-lawsuit.

66. إيوين ماكآسكل (9 سبتمبر 2013). صحيفة الغارديان. مقال: «قضية من «ياهوو» ضد طلبات «وكالة الأمن القومي» لبيانات المستخدم».
Guardian,
http://www.theguardian.com/world/2013/sep/09/yahoo-lawsuit-nsa-surveillance-requests

كريـغ تيمبرغ (11 سـبتمبر 201). صحيفة واشـنطن بوسـت. مقـال: «الحكومة الأميركيّـة هددت بفرض غرامات ضخمة ما لم يعطها «ياهوو» بياناته».
Washington Post,

http://www.washingtonpost.com/business/technology/us-threatened-massive-fine-toforce-yahoo-to-release-data/2014/09/11/38a7f69e-39e8-11e4-9c9f-ebb47272e40e_story.html.

67. ســايروس فاريفار (5 نوفمبر 2013). موقع «آرس تكنيكا» مقال: «في موقف صلب حيال الخصوصيّة، «آبل» تنشر تقارير نادرة عن «عصافير المذكّرات»».

Ars Technica,
http://arstechnica.com/tech-policy/2013/11/apple-takes-strong-privacy-stance-in-new-report-publishes-rare-warrant-canary

68. في الواقــع، اختفــت «عصافير المذكرات» من تقارير «آبل» التي تلت التقريــر الذي أطلق تلك العبارة. ولا يعرف أحد ما المقصود من تلك العبارة على وجه التحديد. جيف جون روبرتس (18 ســبتمبر 2014). مقال: «اختفاء «عصافير المذكرات» من تقارير «آبل»، ما يوحي بضغوط متذرّعة بــ«قانون باتريوت»».
https://gigaom.com/2014/09/18/apples-warrant-canary-disappears-suggesting-new-patriot-act-demands.

69. تحتفظ «مؤسّســة الحدود الإلكترونيّة» بالســجل القياسي في ذلك المجال. نايت كاردوزو وباركر هيغنز وكيرت أوبساهل (13 مارس 2014) تقرير: «تحديث: تشفير التقرير عن الــويب»: من يفعل ماذا».
https://www.eff.org/deeplinks/2013/11/encrypt-web-report-whos-doing-what

70. شــون غالاهــار (6 نوفمبر 2013). موقع «آرس تكنيكا». مقال: «تقنيّــو «غوغل» يقلبون ظهر المجن لــ«وكالة الأمن القومي»، ويشفّرون شبكته الداخليّة».

Ars Technica,
http://arstechnica.com/information-technology/2013/11/googlers-say-f-you-to-nsa-company-encrypts-internal-network.

71. بارتون غيلمان وآشكان سلطاني (14 أكتوبر 2013). صحيفة واشنطن بوست. مقال: «تجمع «وكالة الأمن القومي» ملايين دفاتر العناوين في البريد الإلكتروني عالميّاً».

Washington Post,
http://www.washingtonpost.com/world/national-security/nsa-collects-millions-of-email-address-books-globally/2013/10/14/8e58b5be-34f9-11e3-80c6-7e6dd8d22d8f_story.html

72. اندريا بيترســون وبارتون غيللمان وآشكان ســلطاني (14 أكتوبر 2013). صحيفة واشنطن بوست. مقال: «أخيراً، «ياهوو» يعتمد بروتوكول «إس إس آل» في بريد مستخدميه على الــويب»».

Washington Post,
http://www.washingtonpost.com/blogs/the-switch/wp/2013/10/14/yahooto-make-ssl-encryption-the-default-for-webmail-users-finally.

73. كريغ تيمبرغ وبارتون غيللمان وآشكان سلطاني (26 نوفمبر 2013). صحيفة واشنطن بوست. مقال: «بعد ارتيابها في تجسّــس «وكالة الأمن القومي» عليها، «مايكروســوفت» تسّرع جهود تشفير الحراك الإلكتروني على الإنترنت».

Washington Post,
http://www.washingtonpost.com/business/technology/mic rosoft-suspecting-nsa-spying-to-ramp-up-efforts-to-encrypt-its-internet-traffic/2013/11/26/44236b48-56a9-11e3-8304-caf30787c0a9_story.html

74. هناك أمثلة عدّة. داني ياردون (3 يونيو 2014). صحيفة وول ستريت جورنال. مقال: «شركة «كومكاست» تشفير البريد الإلكتروني توخياً للأمن».

Wall Street Journal,
http://online.wsj.com/articles/comcast-to-encrypt-email-for-security-1401841512.

مايــك كامبــل (13 يونيو 2014). موقع «آبل إنســايدر». مقال: «شركة «آبل» تســعى لتشــفير الإيميل في «آي كلاود»، أثناء تنقله بين مقدّمي خدمة الإنترنت».

Apple Insider,

http://appleinsider.com/articles/14/06/13/apple-will-soon-encrypt-icloud-emails-in-transit-between-service-providers-

75. نايت كاردوزو وباركر هيغنز وكيرت أوبساهل (13 مارس 2014) تقرير: «تحديث: تشفير التقرير عن الـ«ويب»: من يفعل ماذا».
https://www.eff.org/deeplinks/2013/11/encrypt-web-report-whos-doing-what
كلير كاين ميللر (13 يونيو 2013). صحيفة نيويورك تايمس. مقال: «قرار سري لمحكمة يضع شركات التكنولوجيا في قيود البيانات».
New York Times,
http://www.nytimes.com/2013/06/14/technology/secret-court-ruling-put-tech-companies-in-databind.html.

76. في أواخر 2014، عدّلت «آبل» نظام عملها، فبات كل شيء لديها مشفّراً. وتحتوي هواتف الـ«آندرويد» مزايا تشفيريّة منذ 2011، لكن «غوغل» لم يعتمدها كأساس لأعمال تلك الهواتف إلا في 2014، كي ينافس «آبل».
ديفيد سانغر وبرايان شين (26 سبتمبر 2014). صحيفة نيويورك تايمس. مقال: «بداية حقبة ما بعد سنودن: هواتف «آي فون» تغلق أبوابها بوجه «وكالة الأمن القومي»».
New York Times,
http://www.nytimes.com/2014/09/27/technology/iphone-locks-outthe-nsa-signaling-a-post-snowden-era-.html

77. «غوغل» (3 يونيو 2014). المدوّنة الإلكترونيّة الرسميّة لـ«غوغل». وثيقة: «تقرير الشفافية: حماية الإيميل أثناء ترحاله في الإنترنت».
Google Official Blog,
http://googleblog.blogspot.com/2014/06/transparency-report-protecting-emails.html

78. كلير كاين ميللر (13 يونيو 2013). صحيفة نيويورك تايمس. مقال: «قرار سري لمحكمة يضع شركات التكنولوجيا في قيود البيانات».
New York Times,
http://www.nytimes.com/2013/06/14/technology/secret-court-ruling-put-tech-companies-in-databind.html.
كريغ تيمبرغ (11 سبتمبر 201). صحيفة واشنطن بوست. مقال: «الحكومة الأميركيّة هددت بفرض غرامات ضخمة ما لم يعطها «ياهوو» بياناته».
Washington Post,
http://www.washingtonpost.com/business/technology/us-threatened-massive-fine-toforce-yahoo-to-release-data/2014/09/11/38a7f69e-39e8-11e4-9c9f-ebb47272e40e_story.html.

79. كيم زيتر (28 أغسطس 2012). مجلة وايرد. مقال: «معركة «تويتر» دفاعاً عن نشطاء حركة «احتلوا وول ستريت»».
Wired,
http://www.wired.com/2012/08/twitter-appeals-occupy-order.
تيفاني كاري (14 سبتمبر 2012). شبكة «بلومبرغ نيوز». مقال: «تحت ختم رسمي، «تويتر» يسلم تغريدات نشطاء حركة «احتلوا وول ستريت»».
Bloomberg News,
http://www.bloomberg.com/news/2012-09-14/twitter-turns-over-wall-street-protester-posts-under-seal.html

80. فيندو غويل وجيمس س. ماكينلي جونيور (26 يونيو 2014). صحيفة نيويورك تايمس. مقال: «بعد إرغامه على تسليم بيانات، «فيسبوك» يرفع دعوى قضائيّة».

81. تبنّت 3 منظمات أهليّة قضيّة «لافابيت» ضد الـ«إف بي آي»، واستطاعت أن تتخذ موقف «صديق المحكمة»، بمعنى أن تكون مستشارة بشكل موثوق في قضيّة ليست طرفاً فيها، ولا مصلحة مباشرة لها منها. كانت

تلـك المنظّمات الثلاث هي: «مؤسّســة الحدود الإلكترونيّــة» (Electronic Frontier Foundation) المعروفة باســمها المختصر «إي أف أف» (EFF) و«الاتّحاد الأميركي للحريّات المدنيّة» (American Civil Liberities Union) المعروفة باسمها المختصر «إيه سي آل يو» (ACLU)، و«الشركة للمسؤولية المحدودة المؤيّدة شعبيّاً» (Empeopled Limited Liability Company). وتوجـد تفاصيـل تلـك القضايا الثـلاث التي رفعت كلها بتاريخ (25 أكتوبر 2013)، على المواقع الإلكترونيّة للمنظّمات الثلاث على الإنترنت.

82. ريبيـكا ماكينـون (2006). منظمة «هيومن رايتس ووتش». تقرير: «السـباق إلى الهاوية: تواطؤ الشركات في الحجب الصيني للإنترنت».

Human Rights Watch,
http://www.hrw.org/reports/2006/china0806/5.htm

83. توماس لي (25 مايو 2014). صحيفة ســان فرانسيســكو كرونيكل. مقال: «تنبّه إلى عملك: شركات التقنية تتلكأ في استخدام عضلاتها».

San Francisco Chronicle,
http://www.sfgate.com/technology/article/Mind-Your-Business-Slow-flex-of-tech-s-lobbying-5504172.php.

جوزيـف مِنـن (5 يونيو 2014). وكالـة «رويترز» للأنباء. مقـال: «شركات التكنولوجيـا الأميركية تعزز أمن المعلومات لخنق التجسّس العام».

Reuters,
http://www.reuters.com/article/2014/06/05/us-cybersecurity-tech-idUSKBN0EG2BN20140605.
Reform Government Surveillance (2014),
https://www.reformgovernmentsurveillance.com

84. زاك ويتكر (4 شـباط 2013). شـبكة «زد نت». مقـال: «مجموعات الدفاع عن الخصوصيّة تناشـد الحكومة الأميركيّة التوقّف عن ممارسة ضغوط ضد إصلاح قانون البيانات في الاتحاد الأوروبي».

ZDNet,
http://www.zdnet.com/privacy-groups-call-on-us-government-to-stop-lobbyingagainst-eu-data-law-changes-7000010721.

ديفيد ماير (12 مارس 2014). موقع شركة «جيغاوم». مقال: «شركات الـ«ويب» تواجه مجموعة جديدة من القوانين الصارمة بشأن الخصوصيّة في أوروبا: إليكم ما يجب توقّعه».

Gigaom,
http://gigaom.com/2014/03/12/web-firms-face-a-strict-new-set-of-privacy-rulesin-europe-heres-what-to-expect.

85. تيم بيرنرز- لي (ديسمبر 2010). مجلة ساينتفك أميركان. مقال: «يحيا الـ«ويب»».

Scientific American,
http://www.cs.virginia.edu/~robins/Long_Live_the_Web.pdf.

86. جيمـا كيس (11 مارس 2014). صحيفة الغارديان. مقال: «نحو «ماغنا كارتا» للإنترنت: بيرنز- لي يدعو إلى وثيقة حقوق للـ«ويب»».

Guardian,
http://www.theguardian.com/technology/2014/mar/12/online-magna-carta-berners-lee-web.

87. توماس هوبز (1651). دار «أندرو كوكس». كتاب: **ليفياثان**.

http://www.gutenberg.org/files/3207/3207-h/3207-h.htm

88. جون لوك (1690). دار «آونشام تشرتشل». كتاب: **مبحثان للحكم**.

http://books.google.com/books/?id=LqA4nQEACAAJ.

89. الصـوت العام (3 نوفمبر 2009). «إعلان مدريد للخصوصيّة» (2009). «المؤتمر الدولي لمفوّضي الخصوصيّة وحماية البيانات»، مدريد، إسبانيا.
http://privacyconference2011.org/htmls/adoptedResolutions/2009_Madrid/2009_M1.2.pdf

90. ريبيكا ماكينون (2012). كتاب: موافقة المتّصلين بالشبكات.
http://www.owlasylum.net/owl_underground/social/ConsentoftheNetworked.pdf.

الفصل 15: حلول للبقيّة منا

1. إيبين موغلن (27 مايو 2014). صحيفة الغارديان. مقال: «الخصوصيّة تتعرّض للهجوم: وثائق «وكالة الأمن القومي» تكشف تهديدات جديدة للديمقراطيّة».
Guardian,
http://www.theguardian.com/technology/2014/may/27/-sp-privacy-under-attack-nsa-files-revealed-new-threatsdemocracy.

2. وضع عالِم الاجتماع غاري ماركس تصنيفاً يتضمّن 14 طريقة تمكّن الناس من مقاومة الرقابة؛ واعتمدتُ على تصنيفه في هذا الفصل. غاري ت. ماركس (مايو 2003). مجلة جورنال أوف سوشال إيشوز. بحث: «ضربة على الحذاء: ملاشاة الرقابة الجديدة ومقاومتها».
http://web.mit.edu/gtmarx/www/tack.html

3. آر. جاسـون كرونك (25 نوفمبر 2013). موقع «برايفسي مافريك». مقال: «أفكار حول عبارة «تقنيّات تعزيز الخصوصيّة»».
Privacy Maverick,
http://privacymaverick.com/2013/11/25/thoughts-on-the-term-privacy-enhancing-technologies.

4. جـون برودكـين (2 مايو 2014). موقع «آرس تكنيـكا». مقال: «مكوّن إلكتروني للاتصـال بالإنترنت صنعته «مؤسّسة الحدود الإلكترونيّة» بهدف إرغام المواقع الشبكيّة على عدم تتبّع مستخدمي الإنترنت».
«EFF 'Privacy Badger' plugin aimed at forcing websites to stop tracking users,» *Ars Technica*,
http://arstechnica.com/information-technology/2014/05/eff-privacy-badger-plugin-aimed-at-forcing-websites-to-stop-tracking-users

5. «مؤسّسـة الحدود الإلكترونيّة» (2014). تقرير: «دليل إرشادي على الإنترنت من «مركز معلومات الخصوصيّة الإلكترونيّة» بخصوص الأدوات العملية في حماية الخصوصيّة».
http://epic.org/privacy/tools.html.

6. سـارة م. واتسون (16 سـبتمبر 2014). قناة «الجزيرة» وموقعها الإلكتروني. مقال: «اسأل جهاز فك تشفير قنوات التلفزيون: التربص بالضربات».
Al Jazeera,
http://america.aljazeera.com/articles/2014/9/16/the-decoder-stalkedbysocks.html

7. شركة «مايكروسوفت» (21 أغسطس 2013). تقرير: «نظرة عامة على برنامج «بيت لوكر»».
http://technet.microsoft.com/en-us/library/hh831713.aspx.

8. شركة «آبل» (أغسطس 2012). تقرير: «أفضل السُبُل في توظيف «فايل فولت 2.0»».
http://training.apple.com/pdf/WP_FileVault2.pdf.

9. جيمـس ليـن (29 مايو 2014). مجلة فوربس. مقال: «برنامج التشـفير «تروكريب» يختفي في سـحابة من الأسرار».
Forbes

http://www.forbes.com/sites/jameslyne/2014/05/29/open-source-crypto-truecrypt-disappearswith-suspicious-cloud-of-mystery.

10. نيكيتا بوريســوف وإيان غولدبــرغ وإريك بريوار (28 أكتوبر 2004). منتدى في واشــنطن عن «الخصوصيّة في المجتمع الإلكتروني». ورقة بحث: «محادثات غير قابلة للتســجيل، أو، لماذا لا تســتعمل برنامج «خصوصيّة معقولة جدّاً» (*Pretty Good Privacy*) [اختصاراً «بي جي بي» *PGP*]؟».

11. ســتيفان ســوموغي (3 يونيو 2014). مدوّنة إلكترونيّة «غوغل ســيكيورتي أون لاين». تقرير: «تسهيل عملية تشفير التواصل بين نقطتي الإرسال والتلقي».

Google Online Security Blog,
http://googleonlinesecurity.blogspot.com/2014/06/making-end-to-end-encryption-easier-to.html

12. تيم ديركز وإريك رســكورلا (17 أبريل 2014). موقع «قوة المهمة بشــأن هندســة الإنترنت». تقرير: «النسخة 1.3 من «ترانسبورت لاير سكيوريتي»».

http://tools.ietf.org/html/draft-ietf-tlsrfc5246-bis-00.

13. «مؤسّسة الحدود الإلكترونيّة» (2014). تقرير: «إتش تي تي بي إس إيفري وير».

https://www.eff.org/Https-everywhere

14. ثمة دليل إرشــادي جيّد. «مركز معلومات الخصوصيّة الإلكترونيّة» (2014). دليل إرشــادي على الإنترنت من «مركز معلومات الخصوصيّة الإلكترونيّة» بخصوص الأدوات العملية في حماية الخصوصيّة».

http://epic.org/privacy/tools.html.

15. بيتر برايت ودان غودن (14 يونيو 2013). موقع «آرس تكنيكا». مقال: «بريد إلكتروني مشفّر: كم من العناء تحتمل لقاء إبعاد «وكالة الأمن القومي» عنك؟».

Ars Technica,
http://arstechnica.com/security/2013/06/encrypted-e-mail-how-much-annoyance-will-you-tolerate-to-keep-the-nsa-away.

16. يتضمــن النــص التالي رأي «قوة المهمة لهندســة الإنترنت» عن الخصوصيّة والترصّد الواســع. مدوّنة إلكترونيّة لـ«قــوة المهمة لهندســة الإنترنت». جاري آركو وســتيفان فاريل (7 ســبتمبر 2014). تقريــر: «الخصوصيّة والترصّد الواسع».

«Security and pervasive monitoring,» Internet Engineering Task Force,
https://www.ietf.org/blog/2013/09/security-and-pervasive-monitoring

17. آندي غرينبرغ (21 مايو 2014). مجلة وايرد. مقال: «تطبيق مجاني يتيح لســنودن المســتقبل إرسال ملفات ضخمة بأمان مع إغفال الهويّة».

Wired,
http://www.wired.com/2014/05/onionshare.

18. ميريمــير [مجلة عن برنامج لعــزل الخوادم يســتخدمه الــ«هاكرز»] (2014). مقــال: «خصوصيّة متطوّرة وإغفال الهويّة باستخدام برامج «في أم أس» و«في بي آن» و«تور» وغيرها».

IVPN,
https://www.ivpn.net/privacy-guides/advanced-privacy-and-anonymity-part-1.

19. معظــم الثلاجــات الحديثة لا تتمتع بهياكل معدنيّــة صلدة، ولا تصلح لمهمة عزل الموجات الكهرومغناطيســيّة الصادرة عن الخلوي. دقق في موديل ثلاجتك قبل أن تستخدمها لذلك الغرض.

20. جون فاريبه (16 أبريل 2014). موقع «نياتوراما». مقال: «ما هي الوظيفة التي لا توجد إلا في بلدك؟».

Neatorama,
http://www.neatorama.com/2014/04/16/What-Is-a-Job-That-Exists-Only-in-Your-Country

21. روبنسون ماير (24 يوليو 2014). مجلة آتلانتيك. مقال: «تمويه وجهك ليكون مضاداً للرقابة».

Atlantic,
http://www.theatlantic.com/features/archive/2014/07/makeup/374929.

جوزيف كوكس (14 سبتمبر 2014). موقع «كيرنل». مقال: «صعود الحركة المضادة لتقنيّات التعرّف إلى الوجه».

Kernel,
http://kernelmag.dailydot.com/issue-sections/features-issue-sections/10247/anti-facial-recognition-movement.

22. آدم هارفي (2013). «أردية شبحيّة».
http://ahprojects.com/projects/stealth-wear

23. يحتوي المقال التالي قائمة عن تلك التقنيات. فِن برنتون وهيلين نيسـمباوم (2 مايو 2011). صحيفة **فرسـت مونداي الإلكترونيّة**. مقال: «مقاومة عاميّة لجمع البيانات وتحليلها: نحو نظرية سياسيّة لتعمية المعلومات».
First Monday 15,
http://firstmonday.org/article/view/3493/2955.

24. تظهر الخدعة عينها في رواية روبرت أ. هاينلاين **نجمة مزدوجة** (1956). دار «دوبل داي».
http://books.google.com/books?id=bnoGAQAAIAAJ.

25. دانـا بويد (7 نوفمبر 2011). صحيفة **فرسـت مونـداي الإلكترونيّة**. مقال: «لماذا يشـجّع الآباء أطفالهم على مخادعة «فيسبوك» بشأن العمر: آثار غير مقصودة مقصود لـ«قانون حماية خصوصيّة الأطفال»».
First Monday 16,
http://firstmonday.org/ojs/index.php/fm/article/view/3850/3075.

26. مـن المهم التغلّب على ذلك الاسـتهجان. هناك قصة عن مسـتخدم رفض أن يعطي موقع «كومكاسـت» سـبباً لخروجـه مـن خدمـة ذلك الموقـع. في البداية، يبدو الأمـر فظّاً. لكن، إذا أمعنـت التفكير في الأمـر، يتبيّن لك أن «كومكاسـت» ليس مخوّلاً الحصول على تلك المعلومة. زيني جاردن (14 يوليو 2014). موقع «بوينغ بوينغ». مقال: «أصغ إلى «كوماكست» مضطهداً لريان بلوك وفيرونيكا بلمونت، أثناء محاولتهما إلغاء الخدمة».
Boing Boing,
http://boingboing.net/2014/07/14/listen-to-comcast-torture-ryan.html.

27. وضعـت جوليـا أنغويـن كتاباً ممتـازاً عن تجربتهـا في التملّص من الرقابـة في عصر الإنترنـت. جوليا أنغوين (2014). دار «تايمس بوك». كتاب: **الأمة في شبكة الصيد: الرغبة في الخصوصيّة، الأمن والحريّة في عالم الرقابة التي لا تكل.**
Times Books,
http://books.google.com/books?id=bbS6AQAAQBAJ.

28. أثار سـتيوارت باركر هذه النقطة. سـتيوارت أ. باركر (29 أكتوبر 2013). شهادة أمام اللجنة المنتقاة الدائمة بشأن الاستخبارات الأميركيّة في مجلس النواب. «إصلاحات ممكنة لقانون الاستخبارات الأجنبيّة».
Representatives,
http://intelligence.house.gov/sites/intelligence.house.gov/files/documents/Baker10292013.pdf

29. ديفيد سـانغر (13 أغسـطس 2013). صحيفـة **نيويورك تايمس**. مقـال: «التسريبات بشـأن «وكالة الأمن القومي»، تخفض إمكان وضع خطة للدفاع السبراني».
New York Times,
http://www.nytimes.com/2013/08/13/us/nsa-leaks-make-plan-for-cyberdefense-unlikely.html

30. دي. آل. إيه بايبر (7 مارس 2013). دراسة «قوانين حماية البيانات في العالم».
http://files.dlapiper.com/files/Uploads/Documents/Data_Protection_Laws_of_the_World_2013.pdf

31. في العـام 2014، جرّبت «مايكروسـوفت» تحدي طلب أميركي حكومي بشـأن بيانـات للشركة مخزّنة حصرياً في إيرلندا. وطلبت المحكمة من «مايكروسـوفت» تسـليم بياناتها إلى الحكومة الأميركيّـة. وما زال القرار معلّقاً بانتظار حكم الاسـتئناف. جوزيف أكس (31 يوليو 2014) وكالة «رويـترز» للأنباء. مقال: «محكمة أميركيّة تطلب من «مايكروسوفت» تسليم رسائل بريد إلكتروني لمستخدمين، آتية من الخارج».
Reuters,
http://www.reuters.com/article/2014/07/31/usa-techwarrants-idUSL2N0Q61WN20140731

32. صحيفة الغارديان (19 سبتمبر 2014). مقال: «منح سفير بريطاني سابق في الولايات المتحدة، نفاذاً إلى البيانات».

Guardian,
http://www.theguardian.com/technology/2014/sep/19/sir-nigel-shienwald-data-access-role-david-cameron

33. ريتش موغول (25 يونيو 2014). مجلة ماك وورلد. مقال: «لماذا تهتم «آبل» فعليّاً بخصوصيّتك»؟
Macworld,
http://www.macworld.com/article/2366921/why-apple-really-cares-about-your-privacy.html

تشارلز آرثر (18 سبتمبر 2014). صحيفة الغارديان. مقال: «تيم كوك، رئيس «آبل»، يهاجم «غوغل» و«فيسبوك» بسبب ثغرات في الخصوصيّة».

Guardian,
http://www.theguardian.com/technology/2014/sep/18/apple-tim-cook-google-facebook-privacy-surveillance.

34. تتيح البلدان الأوروبيّة لحكوماتها نفاذاً أوسع كثيراً إلى البيانات، بالمقارنة مع الولايات المتحدة. سايروس فاريفار (13 أكتوبر 2013). موقع «آرس تكنيكا». مقال: «أوروبا لن تنقذك: لماذا ربما يكون بريدك الإلكتروني أكثر أماناً في الولايات المتحدة».

Ars Technica,
http://arstechnica.com/tech-policy/2013/10/europe-wont-save-you-why-e-mail-is-probably-safer-in-the-us

35. جيمس كانتر (8 أبريل 2014). صحيفة نيويورك تايمس. مقال: «حمايةً للخصوصيّة، المحكمة الأوروبيّة ترفض قوانين تخزين البيانات».

New York Times,
http://www.nytimes.com/2014/04/09/business/international/european-court-rejects-data-retention-rules-citing-privacy.html.

36. ديفيد ماير (17 يوليو 2014). مقال: «صار القانون «الطارئ» البريطاني «دريب» للرقابة أمراً واقعاً الآن».
http://gigaom.com/2014/07/17/the-uks-emergency-drip-surveillance-law-is-now-a-done-deal

37. راي كوريغان (11 يوليو 2014). مقال: «الرقابة العامة والساسة المذعورون».
http://b2fxxx.blogspot.com/2014/07/masssurveillance-and-scared-politicians.html.

38. من بينها مواقع «نو سي سي تي في»
http://www.no-cctv.org.uk/camera_locations/default.asp

و«سي سي تي في تراجر هانت»

http://cctvtreasurehunt.wordpress.com.

و«إن واي سي سيرفالنس كاميرا بروجكت»

http://www.mediaeater.com/cameras.

39. كريستيان (24 يونيو 2004). موقع «جنبو» الإلكتروني. مقال: «عقب تظاهرات ضخمة السبت ضد قانون «إن إي آي إس» (*NEIS*)، حكومة كوريا الجنوبيّة تبرهن على تفهّمها للديمقراطيّة».

Jinbo,
http://act.jinbo.net/drupal/node/5819.

سيونغ كيم وسونهو كيم (أكتوبر 2004). مقال: «الصراع على استخدام تقنيات المعلوماتية في المدارس الكوريّة».

http://ajou.ac.kr/~seoyong/paper/Seoyong%20Kim-2004-The%20Conflict%20Over%20the%20Use%20of%20Information%20Technology.pdf.

40. شركة «آي بي أم» (16 كانون أول 2004). تقرير: «مخزن «فيوتشر ستور» التابع لمجموعة «مترو»، يصدم الجمهور العام في ألمانيا- بفضل التكنولوجيا اللاسلكيّة».

ftp://ftp.software.ibm.com/software/solutions/pdfs/10704035_Metro_cs_1b.pdf.

كيم زيتر (28 فبراير 2004). مجلة وايرد. مقال: «الألمان يحتجّون على خطط لصنع هويّات بالموجات اللاسلكيّة لهم».

Wired,

http://archive.wired.com/techbiz/media/news/2004/02/62472.

41. ك. س. جونز (17 فبراير 2009). مجلة إنفورمايشن ويك. مقال: «شروط جديدة من «فيسبوك» تثير احتجاجاً».

Information Week,

http://www.informationweek.com/software/social/facebooks-terms-of-use-draw-protest/d/d-id/1076697.

بوبي جونسون وآفوا هيرش (18 فبراير 2009). صحيفة الغارديان. مقال: «فيسبوك» يتراجع عقب احتجاجات شبكيّة».

Guardian,

http://www.theguardian.com/technology/2009/feb/19/facebook-personal-data

42. آشلي هالساي الثالث وديريك كرافتز (25 نوفمبر 2010). صحيفة واشنطن بوست. مقال: «احتجاجات على التفتيش اليدوي من قِبَل «أمن إدارة النقل»، وماسحات الجسد لا تؤخّر رحلات «عيد الشكر»».

Washington Post,

http://www.washingtonpost.com/wp-dyn/content/article/2010/11/24/AR2010112406989.html

43. إنّها فكرة التغيير التراكمي، أو الدفع بالتشويش. شارلز ي. ليندبلوم (ربيع 1959). مجلة بابليك أدمنستريشن ريفيو. مقال: «علم «الدفع بالتشويش»».

الفصل 16: الأعراف الاجتماعيّة ومقايضة «البيانات الضخمة»

1. بول بلومنثال (2 مارس 2009). «مؤسّسة صن لايت». تقرير: «لا يملك الكونغرس وقتاً لقراءة «قانون باتريوت» الأميركي».

Sunlight Foundation,

http://sunlightfoundation.com/blog/2009/03/02/congress-had-no-time-to-read-the-usa-patriot-act.

2. ليونيل هاددي وستانلي فيلدمان (سبتمبر 2011). مجلة أميركان سايكولوجست. مقال: «الأميركيّون يردّون سياسياً على 11/9: فهم تأثير ضربات الإرهاب وعقابيلها».

American Psychologist 66,

http://www.ncbi.nlm.nih.gov/pubmed/21823777.

3. تيم داوسون (9 يونيو 2014). «الاتحاد القومي للصحافيّين [الأميركيّين]». مقال: «أقرب إلى الـ«ستازي» منه إلى جيمس بوند».

National Union of Journalists,

http://www.nuj.org.uk/news/more-like-the-stasi-than-james-bond.

4. جوزيف كامبوس الثالث (7 سبتمبر 2013). جامعة أوكسفورد. «الذاكرة والتذكّر: انتشار الخوف والرعب والإرهاب، في التحكّم والشرعيّة».

http://www.inter-disciplinary.net/at-the-interface/wp-content/uploads/2013/07/camposfhtpaper.pdf

5. جاك غولد سميث (9 أغسطس 2013). مدوّنة إلكترونيّة «لوفير». مقال: «تأمّلات عن الإشراف على «وكالة الأمن القومي» مع توقّع أنّ سلطات «وكالة الأمن القومي» (والإشراف والشفافيّة) سوف تتوسّع».

Lawfare,

http://www.lawfareblog.com/2013/08/reflections-on-nsaoversight-and-a-prediction-that-nsa-authorities-and-oversight-and-transparencywill-expand.

6. دونـا ج. بيـير- موندي (أغسـطس 2009). «جامعة هـاواي» في «مانوا». كتـاب: **عن الإرهابيّـين والطغاة والاضطـراب الاجتماعي: نموذج نظري عـن تنافس المخاوف لتطوير قانـون يتّصل بالخصوصيّة في الاتصالات بمواجهة رقابة قوى إنفاذ القانون الأميركيّة.**

University of Hawai'i at Manoa,
http://books.google.com/books?id=8LveYgEACAAJ

كيفـن ج. روبي (2012). مطبعة جامعة شـيكاغو. كتاب: **المجتمع والدولـة والخوف: إدارة الأمن القومي والحدود بين الذعر والرضى عن الذات.**

University of Chicago Press,
http://books.google.com/books?id=UPILnwEACAAJ.

7. داون روثه وسـتيفن موزاتي (نوفمبر 2004). مقال: «الأعداء في كل مكان: الإرهاب والذعر الأخلاقي والمجتمع المدني الأميركي».

http://www.researchgate.net/publication/227209259_Enemies_Everywhere_Terrorism_Moral_Panic_and_US_Civil_Society/file/32bfe50d3c7fe0d03b.pdf

ديفيد روثكوبف (6 أغسطس 2013). مجلة **فورين آفيرز**. مقال: «أخطار حقيقيّة».

Foreign Policy,
http://www.foreignpolicy.com/articles/2013/08/06/the_real_risks_war_on_terror

8. إنّـه الأمن على مدار السـنة. بروس شـناير (22 فبراير 2007). مجلة **وايرد**. مقـال: «لماذا يأتي رجال الشرطة الأذكياء أموراً غبيّة؟».

Wired,
http://archive.wired.com/politics/security/commentary/securitymatters/2007/02/72774.

9. في الوثائق المسّربة من «وكالة الأمن القومي»، هناك أقوال تشير تحديداً إلى 9/11: «أنا أفضّل أن أكون هنا اليوم لأشرح هذه البرامج، على أن أشرح حادثاً آخر يشـابه 9/11 لم نكن قادرين على منعه». جاسـون ليوبولد (30 أكتوبـر 2013). قناة «الجزيرة» التلفزيونيّة. مقال: «كُشِـف أخيراً: اسـتخدمت «وكالـة الأمن القومي» حادث 9/11 كمفتاح صوتي في تبرير رقابتها».

Al Jazeera,
http://america.aljazeera.com/articles/2013/10/30/revealed-nsa-pushed911askeysoundbitetojustifysurveillance.html.

10. كلاي شـيركي (14 مارس 2010). ملاحظات في برنامج تلفزيوني في «أوستن» بولاية تكساس، اقتبسها كيفن كيلي (2 أبريل 2010) في مقال: «مبدأ شيركي».

Kevin Kelly,
http://kk.org/thetechnium/2010/04/the-shirky-prin.

11. جاك غولد سميث (9 أغسطس 2013). مدوّنة إلكترونيّة «لوفير». مقال: «تأمّلات عن الإشراف على «وكالة الأمن القومي» مع توقّع أنّ سلطات «وكالة الأمن القومي» (والإشراف والشفافيّة) سوف تتوسّع».

Lawfare,
http://www.lawfareblog.com/2013/08/reflections-on-nsaoversight-and-a-prediction-that-nsa-authorities-and-oversight-and-transparencywill-expand.

12. أعتقد شخصيّاً بأن الناس في كوبا وكوريا الشمالية في مأمن من الإرهاب، ولكن بأي ثمن؟

13. بـروس شـناير (17 مايو 2007). مجلـة **وايرد**. مقال: «دروس مـن الهجوم في «جامعـة فرجينيا»: المخاطر النادرة تولّد ردود أفعال لا عقلانيّة».

Wired,
http://archive.wired.com/politics/security/commentary/securitymatters/2007/05/securitymatters_0517

14. ترجع العبارة إلى أوقات قديمة، وجاءت ضمن قرار من «المحكمة العليا»: «ليس أننا نختار بين الحريّة والنظام،

بـل نختار بين الحرية مـع النظام من جهة، والفوضى من كليهما من الجهـة الثانية. هناك خطر من عدم قيام المحكمـة بمزج منطقها القانوني مع شيء من الحكمة الآتية من الممارسـة، في تحويـل «وثيقة حقوق المواطن» الدستوريّة إلى حلف انتحاري». قرار من «المحكمة العليا» (16 مايو 1949).
http://caselaw.lp.findlaw.com/scripts/getcase.pl?court=us&vol=337&invol=1.

15. يوجد كتاب اسـتقى عنوانه من تلك العبارة. ريتشـارد أ. بوسـنر (2006). مطبعة جامعة أوكسـفورد. كتاب: **ليس حلفاً انتحارياً: الدستور في زمن الطوارئ القوميّة.**
Oxford University Press,
http://books.google.com/books?id=hP6PAAAAMAAJ.

16. ريتشـارد أورانج (14 أبريـل 2012). صحيفة الغارديـان. مقال: «الرد على الكراهيـة بالحب: كيف حاولت النرويج التغلّب على الذعر الذي سببه أندرياس بريفيك».
Guardian,
http://www.theguardian.com/world/2012/apr/15/anders-breivik-norway-copes-horror

تيـم كوشـينغ (26 يوليو 2012). موقـع «تيك درت». مقال: «بعد سـنة من مجزرة بريفيـك، تتابع النرويج مكافحة الإرهاب بالديمقراطية والانفتاح والحب».
Tech Dirt,
https://www.techdirt.com/articles/20120724/20363519819/one-year-after-breivik-massacre-norway-continues-to-fight-terrorismwith-democracy-openness-love.shtml

17. بروس شناير (7 يناير 2012). موقع «إيه أو آل نيوز». مقال: «رد فعلنا هو الفشل الحقيقي للأمن».
AOL News,
https://www.schneier.com/essays/archives/2010/01/our_reaction_is_the.html

18. جون موللر ومارك ستيوارت (2011). «مطبعة جامعة أوكسفورد». كتاب: **إرهاب، أمن ونقود: التوازن بين المخاطر والفوائد والتكاليف في وزارة الأمن الوطني.**
Oxford University Press, chap. 2,
http://books.google.com/books?id=jyYGL2jZBC4C

19. حتى إنني آلّفت كتاباً بهذا العنوان. بروس شناير (2003). دار «ويلي» للنشر. كتاب: **ما وراء التفكير بتعقّل عن الأمن في عالم يغيب غير مستقر.**
Wiley,
http://books.google.com/books/about/?id=wuNImmQufGsC.

20. تحاجج أسـتاذة القانـون في «جامعة نيويورك» هيلين نسـينباوم، بأنّ الخصوصيّة لا تفهم إلا ضمن السـياق والتوقّعات. هيلين نسينباوم (خريف 2011). دراسة: «مقاربة سياقيّة للخصوصيّة على الإنترنت».
http://www.amacad.org/publications/daedalus/11_fall_nissenbaum.pdf

آليكـس مادريغـال (29 مارس 2012). مجلة آتلانتيك. مقال: «الفيلسـوف الذي ترك بصماته على السياسـة الجديدة لـلجنة التجارة الفيدرالية» بشأن الخصوصيّة».
Atlantic,
http://www.theatlantic.com/technology/print/2012/03/the-philosopher-whose-fingerprints-are-all-over-the-ftcs-new-approach-to-privacy/254365.

21. يعني ذلك أن الفروقات الإقليميّة ستستمر في الإنترنت، على الرغم من أن طبيعتها العالميّة تقتضي انسجاماً أكثر.

22. سـارة غريـدار كرونان ونيل ف. بايلين (5 أبريل 2007). «رابطة المحامـين الأميركيّين». مقال: «هل يجدر بي البحث عن أعضاء هيئة المحلّفين على «غوغل»؟ واعتبارات أخلاقيّة أخرى».
American Bar Association,
http://apps.americanbar.org/litigation/committees/products/articles/0407_cronan.html

23. سامانثا هنيغ (مارس 2013). موقع «غلامور». مقال: «لم يجدر بك التوقّع عن المواعدة عبر «غوغل»؟»
Glamour,

http://www.glamour.com/sex-love-life/2013/03/why-you-should-stop-googling-your-dates.

هناك شريط فيديو يظهر المدى المريب الذي بلغته تلك الأشـياء. ماريـو كونتريراس (29 مايو 2014). «اللقاء في مكان عام».

http://vimeo.com/96870066.

24. اندريا بارتز وبرينا إيهرليش (7 ديسـمبر 2011). شـبكة «سي آن آن». مقال: «ما يجب وما لا يجب في البحث عن الناس على «غوغل»».

CNN,
http://www.cnn.com/2011/12/07/tech/social-media/netiquette-google-stalking.

25. جوي كوسكاريلي (12 ديسمبر 2010). مقال: «هل يملك جوليان أسانج بروفايل على «أوكي كيوبيد»؟»
http://blogs.villagevoice.com/runninscared/2010/12/does_julian_ass.php.

26. مجلة الإيكونومست (5 يونيو 2014). مقال: «تجّار البؤس».

Economist,
http://www.economist.com/news/international/21606307-howshould-online-publication-explicit-images-without-their-subjects-consent-be.

27. ديفيد كرافتس (15 يوليو 2013). مجلة وايرد. مقال: «مواقع إزالة «صور الاعتقال» مدانة بالابتزاز».
Wired,
http://www.wired.com/2013/07/mugshot-removal-extortion.

ديفيد سيغال (6 أكتوبر 2013). صحيفة نيويورك تايمس. مقال: «معتقَل بصور الاعتقال على الإنترنت».
New York Times,
http://www.nytimes.com/2013/10/06/business/mugged-by-a-mug-shot-online.html.

28. ديفيد برين (1998). دار: «بازيك بوكس». كتاب: **المجتمع الشفّاف: هل ترغمنا التكنولوجيا على الاختيار بين الخصوصيّة والحريّة؟**

http://www.davidbrin.com/transparentsociety1.html

29. إميلي نوسباوم (12 فبراير 2007). مجلة نيويورك ماغازين. مقال: «قل كل شيء».
New York Magazine,
http://nymag.com/news/features/27341.

30. جيسي إروين (7 أكتوبر 2014). موقع «موديل فيو كالتشر». مقال: «تهيئة الطلاب لرقابة مدى العمر».
Model View Culture,
http://modelviewculture.com/pieces/grooming-students-for-a-lifetime-of-surveillance

31. تطلـب بعض المدارس من الطلبة ارتداء شـارات إلكترونيّة، وهي التقنية عينها التي يسـتخدمها المزارعون مع قطعان الماشية. وكالة أنباء «أستوشيتدبرس» (11 أكتوبر 2010). مقال: «مدارس في منطقة «هوستون» تتبّع التلامذة بشارات تعمل بالإشارات اللاسلكيّة».

http://www.dallasnews.com/news/education/headlines/20101011-Houston-area-schools-tracking-students-with-6953.ece

32. الأمم المتّحدة (10 ديسمبر 1948). وثيقة: «الإعلان العالمي لحقوق الإنسان».
http://www.un.org/en/documents/udhr

33. جـرت مراجعة الميثـاق في 2010. «المحكمة الأوروبيّة لحقوق الإنسـان» (1 يونيـو 2010). «الميثاق الأوروبي لحقوق الإنسان»، «المجلس الأوروبي».

http://www.echr.coe.int/documents/convention_eng.pdf

34. دوغ ليندر (2014). جامعة ميسوري. بحث: «تقصي التضاربات الدستوريّة: الحق في الخصوصيّة».
http://law2.umkc.edu/faculty/projects/ftrials/conlaw/rightofprivacy.html.

35. الاتحاد الأوروبي (18 ديسمبر 2000). «إعلان الحقوق الأساسيّة في الاتحاد الأوروبي».

http://ec.europa.eu/justice/fundamentalrights/charter/index_en.htm.

36. تعيد الوثيقة التأكيد على «الحق الإنساني في الخصوصيّة، وبموجبها لا يتعرض فرد لتدخّل اعتباطي أو غير شرعي في خصوصيّته أو خصوصيّتها، وكذلك الحال بالنسبة للمنزل والعائلة والمراسلات. ويملك أيضاً الحق في الحماية قانونياً ضد ذلك التدخل. وتقر [الأمم المتحدة] أنّ ممارسة الحق في الخصوصيّة مهم بالنسبة لتحقيق الحق في حرية التعبير، وحرية تبني الأفكار من دون تدخّل، وهو [الحق في الخصوصيّة] من أسس المجتمع الديمقراطي». الجمعية العامة للأمم المتحدة (21 يناير 2014)، قرار تبنّته الجمعية العامة، في 18 ديسمبر 2013، 68/167، «الحق في الخصوصيّة في العصر الرقمي».

http://www.un.org/ga/search/view_doc.asp?symbol=A/RES/68/167.

37. أُعلِنت الشرعة في العام 2000، لكنها لم تكتسب قوة القانون إلا بعد إقرارها جزءاً من «اتفاقيّة لشبونة» في 2009. الاتحاد الأوروبي (18 ديسمبر 2000). «شرعة الحقوق الأساسيّة في الاتحاد الأوروبي».

http://ec.europa.eu/justice/fundamental-rights/charter/index_en.htm.

38. قال الرئيس الأميركي بنجامين فرانكلين: «أولئك الذين يتخلّون عن حريّة أساسيّة ليشتروا القليل من الأمن المؤقت؛ لا يستحقون الحريّة ولا الأمن».

39. مارسيا ستيبانك (8 أغسطس 2013). جامعة ستانفورد. مقال: «تأثير سنودن: فرصة؟»

http://www.ssireview.org/blog/entry/the_snowden_effect_an_opportunity.

40. جيرالد ف. سايب (21 نوفمبر 2008). صحيفة وول ستريت جورنال. مقال: «في الأزمة، هناك فرصة لأوباما».

Wall Street Journal,

http://online.wsj.com/news/articles/SB122721278056345271.

41. بروس شناير (2012). كتاب: **كَذَبَة ومتمردون: تفعيل الثقة التي يحتاجها المجتمع لينمو**. دار «ويلي» للنشر.

http://www.wiley.com/WileyCDA/WileyTitle/productCd-1118143302.html.

42. شارلز سافران وآخرون (يناير/فبراير 2007). مجلة **رابطة المعلوماتيّة الطبيّة الأميركيّة**. بحث: «نحو إطار قومي للاستخدام الثانوي للبيانات الصحيّة: ورقة بيضاء من «رابطة المعلوماتيّة الطبيّة الأميركيّة»».

Journal of the American Medical Informatics Association 14,

https://www.sciencedirect.com/science/article/pii/S106750270600212X.

بيتر جانسن ولارس جانسن وتسورن بروناك (يونيو 2012). مجلة **نايتشر**. بحث: «التنقيب في السجلات الصحيّة: نحو تحسين التطبيقات البحثية والرعاية الطبيّة».

Nature Reviews: Genetics 13,

http://www.dartmouth.edu/~cbbc/courses/bio270/PDFs-13S/Tim_Byounggug.pdf.

43. راينول جونكو (2014). بحث: «انخراط الطلبة عبر الـ«سوشال ميديا»: ممارسات مبنيّة على الأدلة كي تستخدم في العلاقات مع الطلاب».

http://www.wiley.com/WileyCDA/WileyTitle/productCd-1118647459.html.

44. كريستيان رودر (28 يوليو 2014). موقع «أو كيه تريند». مقال: «نحن نجري تجارب على البشر!»

OK Trends,

http://blog.okcupid.com/index.php/we-experiment-on-human-beings

كريستيان رودر (4 سبتمبر 2014). صحيفة وول ستريت جورنال. مقال: «عندما تسترق المواقع الشبكيّة النظر إلى الحياة الخاصة».

Wall Street Journal,

http://online.wsj.com/articles/when-websitespeek-into-private-lives-1409851575.

45. مارك فاينشتاين (4 سبتمبر 2014). صحيفة هافنغتون بوست. مقال: «أوكي كيوبيد» بالأحرى أنه «أوكي غبي».

Huffington Post,

http://www.huffingtonpost.com/mark-weinstein/okcupid-thats-okstupid_b_5739812.html.

46. المكتب التنفيذي للرئيس أوباما (2013). وثيقة: «الحكومة الإلكترونيّة: بناء منصة القرن 21 كي تخدم الشعب الأميركي بصورة أفضل».

http://www.whitehouse.gov/sites/default/files/omb/egov/digital-government/digital-government.html.

شركة «مايكروسوفت» (27 مارس 2013). مركز أنباء «مايكروسوفت». تقرير: «تبني الدولة والحكومات المحليّة تقنيّة «سي آر أم» داينامكس من مايكروسوفت، بهدف الارتقاء بمستوى تقديم الخدمات للمواطن».

Microsoft News Center,

http://www.microsoft.com/en-us/news/press/2013/mar13/03-27dynamicscrmpr.aspx.

47. تبدي «القيادة الحكوميّة للاتّصالات» في بريطانيا، خشيتها علناً من ذلك النقاش. إذ تحدّثت إحدى وثائق سنودن عن محادثات لتجنّب «النقاش العام المؤذي» عن مدى الرقابة. جيمس بول (25 أكتوبر 2013). صحيفة **الغارديان**. مقال: «الكشف عن مذكرات سريّة تبيّن جهود «القيادة الحكوميّة للاتّصالات» للإبقاء على الرقابة العامة سرّاً».

Guardian,

http://www.theguardian.com/uk-news/2013/oct/25/leaked-memos-gchq-mass-surveillance-secretsnowden.

48. عمليّاً، تلك العبارة هي اقتباس لمارتن لوثر كينغ من نص لثيودور باركر، وكان من دعاة إزالة الفوارق العنصريّة، في العام 1835، يرد فيه: «لا أتظاهر بأنني أفهم الكون الأخلاقي؛ لأن قوسه ضخم، فيما لا تتصل عيناي لسوى الطرق الصغيرة. لا أستطيع احتساب القوس بأكمله ومتابعته بتجربة البصر؛ لكني أستطيع تخمينه ضميريّاً. ولكن، استناداً إلى ما أراه، أنا متأكّد أنه يتّجه صوب العدالة». غارسون (15 نوفمبر 2012). **قاموس تقصي الاقتباسات**. «كون الأخلاق له قوس طويل لكنه يتّجه صوب العدالة».

Quote Investigator,

http://quoteinvestigator.com/2012/11/15/arc-of-universe.

الفهرس

-ب-

- ت -

- ث -

- ج -

- ح -

-غ-

-ف-


منتدى العلاقات العربية والدولية